Security Considerations in Mobile and Wireless Computing

6

Learning Objectives

After completing this chapter you will be able to:

- understand the security challenges presented by mobile devices and information systems access in wireless computing environments.
- understand the challenges faced by the mobile work force and their implications for information systems security.
- form an understanding and the challenges presented by the mobile and wireless computing era to certain industry segments such as the credit cards business.
- appreciate a mitigation strategy like the CLEW for possible protection of credit cards users.
- understand cryptographic controls, lightweight directory access protocol (LDAP) for mobile devices, RAS security for mobile devices and networking API security for mobile computing devices.
- learn about security issues brought in by use of media players.
- understand organizational security implications with mobile devices and learn what organizational measures need to be implemented for protecting information systems from threats in mobile computing era.
- understand the use of RFID in mobile commerce appreciating physical security counter-measures to protect thefts of mobile devices.
- understand the security threats and privacy concerns in 'wearable technology'.

6.1 Introduction

In the modern era, the discussion on the topic of security cannot be complete without this topic. This is to the rising importance of *mobile handheld devices, wireless computing, wireless networks*, and the fact that today belongs to *mobile computing*. As the mobility of workers increases, security issues also increase in number, because working with technology outside the office brings many challenges.

In the recent years, the use of laptops, personal digital assistants (PDAs) and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart handheld devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the *smart phone*. Smart phones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. While IT departments of organizations as yet are not swapping employees' company-provided PDAs (as the case may be) for the smart phones, many users may bring these devices from home and use them in the office. Research in Motion's (RIM) Blackberry Wireless

Handheld is an alternate technology. According to RIM report [see the RIM uniform resource locator (URL) quoted in the *Further Reading* section], there are approximately 10,000 corporations that use the Blackberry enterprise server and client/server software for data communication between corporate Blackberry devices and other mail systems. Thus, the larger and more diverse community of mobile users and their devices increases the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

6.2 Proliferation of Mobile and Wireless Devices

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now there is a long list of options ranging from high-end PDAs with integrated wireless modems down to small phones with wireless web-browsing capabilities. Even the simplest of handheld devices provide enough computing power to run small applications, play games, music and make voice calls. A key driver for the growth of mobile solutions for business is the proliferation of handheld devices in the enterprise. Figure 6.1 shows some typical handheld devices.

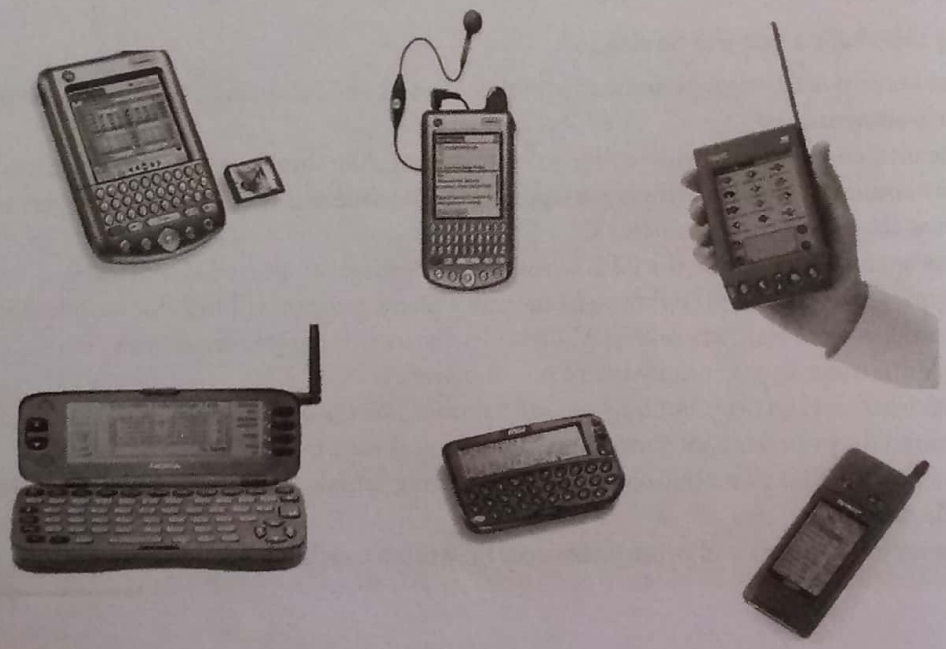


FIGURE 6.1 | Typical handheld devices.

As more personal devices find their way into the enterprise, corporations are realizing security threats that come along with the benefits achieved with mobile solutions. Since the term 'mobile device' includes many products, we first provide a clear distinction among the key terms: mobile computing, wireless computing and handheld devices. Figure 6.2 helps us understand how these terms are related. Wireless refers to the method of transferring information between a computing device, such as a PDA, and a data source, such as an agency database server, without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop, that is not tethered.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication between devices at all. Thus, while 'wireless' is a subset of 'mobile', in most cases, an application can be mobile without being wireless. Smart handhelds are defined as handheld or pocket-size devices that connect to a wireless or cellular network, and can have software installed on them. This includes networked PDAs and smart phones, and in this chapter, the term 'handheld' is used as an all-embracing term.

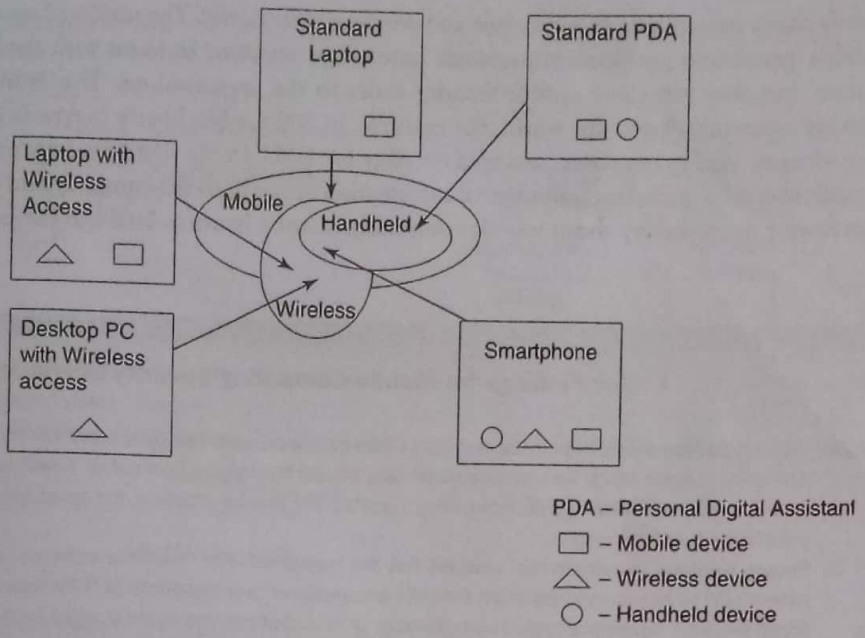


FIGURE 6.2 | Mobile, wireless and handheld devices.

6.3 Trends in Mobility

It is worth noting the trends in mobile computing; this will help readers appreciate the seriousness of security issues in the mobile computing domain. Figure 6.3 shows the different types of mobility and their implications.

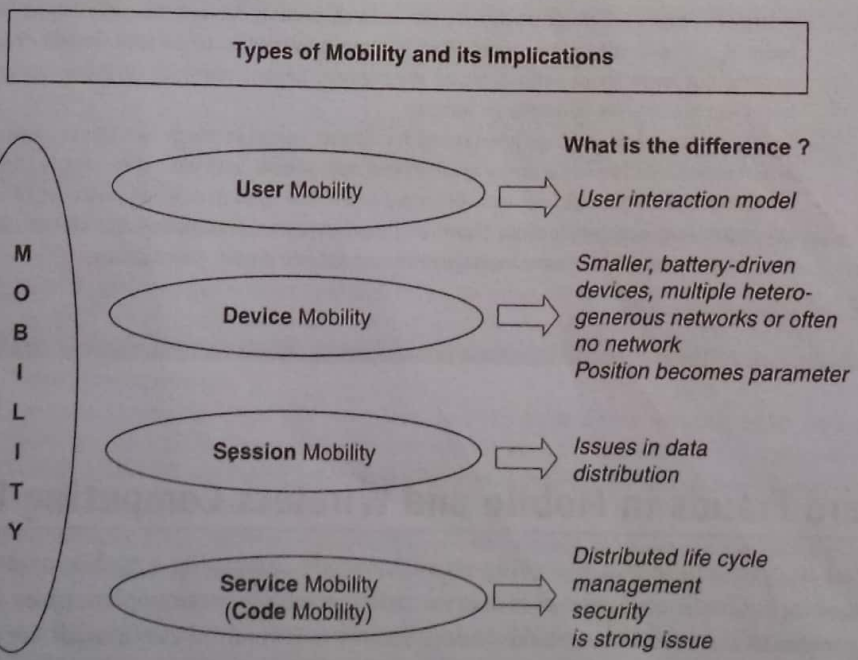


FIGURE 6.3 | Mobility types and implications.

To assess the trend in mobile computing, online interviews have been conducted to identify the major challenges in the mobility domain, and how they are being dealt with by users and IT managers today. In one such survey, reported by Quocirca (www.quocirca.com), of the 2,853 respondents, 29% had a broad experience of wireless laptops, 14% had a broad experience of smart handhelds, with around a further 60% in each case having a more limited or unofficial experience. Findings from surveys

like these help us demystify many perceptions about mobile and wireless connectivity. The results of surveys like these indicate that we are grappling with a 'perception problem'; most people have not as yet come to terms with the fact that the handheld devices may look 'harmless' but they can cause serious security issues to the organizations. This is in spite of the rampant information systems security exposures all over the world. For example, in 2003, a Blackberry (a type of handheld device), that reportedly belonged to a Morgan Stanley employee, was sold on eBay for USD 15.50. The buyer discovered that it contained hundreds of electronic mails (e-mails), including confidential information about both the company and the employee. Box 6.1 shows a few key findings from a recent survey about mobile computing security issues to establish the point just made.

BOX 6.1

Key Findings for Mobile Computing Security Scenario

1. **With usage experience, awareness of mobile users gets enhanced:** Survey showed that those with broad wireless laptop experience place less emphasis on this aspect for the deployment of smart handhelds. However, an experience of small handheld deployment boosted the numbers seeing the need for increased provision of user support and training.
2. **People continue to remain the weakest link for laptop security:** Antivirus software, secured virtual private network (VPN) access and personal firewalls are deployed over two-thirds of IT professionals, but those with a broad wireless experience regard loss, damage or unauthorized use as their major concerns and these depend on the care taken by the users and well-communicated security policies.
3. **Wireless connectivity does little to increase burden of managing laptops:** The cost and complexity of device management is seen as an issue by around half of the IT professionals surveyed. However, the level of challenge perceived to affect security, device management and use support is unaffected by a broader experience of wireless laptop deployment.
4. **Laptop experience changes the view of starting a smart handheld pilot:** The key concerns for starting a smart handheld are security and cost of devices, but these lessen for those with a broad wireless laptop experience. However, the concern over choosing the most appropriate devices rises with experience and the users cite further concerns over interoperability and compatibility.
5. **There is naivety and/or neglect in smart handheld security:** While plenty of emphasis is placed on security, a large number of IT departments do not enforce security for smart handhelds as well as for laptops or they leave it in the hands of the users. This is more prevalent in those with limited or unofficial smart handheld activity, but even those with a broad experience, almost one-third of those surveyed, do not treat smart handheld security as seriously as laptops.
6. **Rules rather than technology keep smart handhelds' usage in check:** Businesses with an existing experience of smart handhelds favored a policy of controlled deployment, with almost two-thirds of those surveyed providing a limited choice of devices, and only one-third of the surveyed population was user of technology solution based on continuous synchronization. However, broad experience increases the use of other automated solutions, such as centralized software management and remote device deactivation.

Courtesy: www.quocirca.com.

6.4 Credit Card Frauds in Mobile and Wireless Computing Era

This is an all new trend in cyber crime that is coming up with mobile computing – mobile commerce (m-commerce) and mobile banking (m-banking). Credit card related frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile handheld devices, factors that result in easy availability of these gadgets to almost anyone. *Mobile credit card transactions* are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.

Today belongs to 'mobile computing', that is *anywhere anytime computing*. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment.

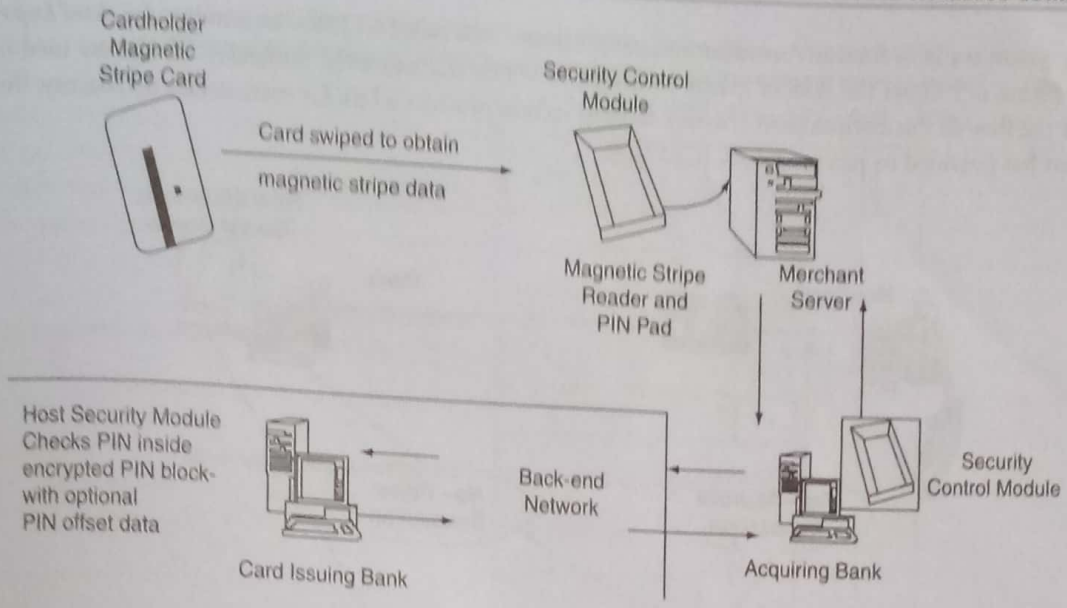


FIGURE 6.4 | Online environment for credit card transactions.

These businesses include mobile utility repair service businesses, locksmiths, mobile windshield repair and others. Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers. Figure 6.4 shows the basic flow of transactions involved in purchases done using credit cards. Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur. But they could reduce ID fraud even more if they gave consumers better tools to monitor their accounts and limit high-risk transactions (Box 6.2).

BOX 6.2

Potential Wireless Users – Beware!

While wireless processing is a very good system for many companies, it is not for all mobile businesses. There are some drawbacks to wireless processing that many potential wireless users should be aware of before they venture into wireless processing:

1. *Wireless processing equipment is expensive.* There is no way to get around this. Wireless credit card machines are the most advanced processing terminals available. You get what you pay for! For a wireless terminal with a printer, expect to pay at least USD 800 for a new terminal, and USD 700 for a refurbished terminal. If you find yourself about to purchase a terminal that is much cheaper than any other you find, it is most likely outdated equipment that uses outdated cellular networks. In other words, it is a scam, and you are about to buy a really expensive paperweight.
2. *Wireless processing comes with extra fees.* Just like a cell phone, wireless credit card machines operate on cellular networks. You have to pay for this cellular service in addition to the high cost of equipment. Luckily wireless fees for processing are nowhere near what they are for cell phones. Expect to pay USD 20–25 per month for a wireless service fee.
3. *Wireless credit card machines are subject to cellular coverage blackouts.* Typical thinking – 'My cell phone works almost everywhere, so my wireless credit card machine will too'. Sadly, this is not the case. Wireless credit card processing uses a business cellular network called the Motient or Mobitex network. Your cell phone may be using a network called code division multiple access (CDMA) or time division multiple access (TDMA) [global system for mobile communications (GSM)] or some other technology-based network. The coverage that your cell phone gets is much greater than the wireless processing network. There can be some states in your country with no coverage for wireless processing at all.
4. *You cannot process checks or debit transactions over a wireless network.* Currently owing to federal regulations, it is impossible to process debit transaction or electronic checks over a wireless network. This is something that will probably end up being allowed in the future, but as of now there is not sufficient security or encryption to process these transactions wireless.

There is a system available from an Australian company 'Alacrity'; it is called CLEW – an acronym for *closed loop environment for wireless*. Figure 6.5 shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment [*Further Reading* section provides a link for more details on Alacrity, the Australian company that has provided its patented work (CLEW)].

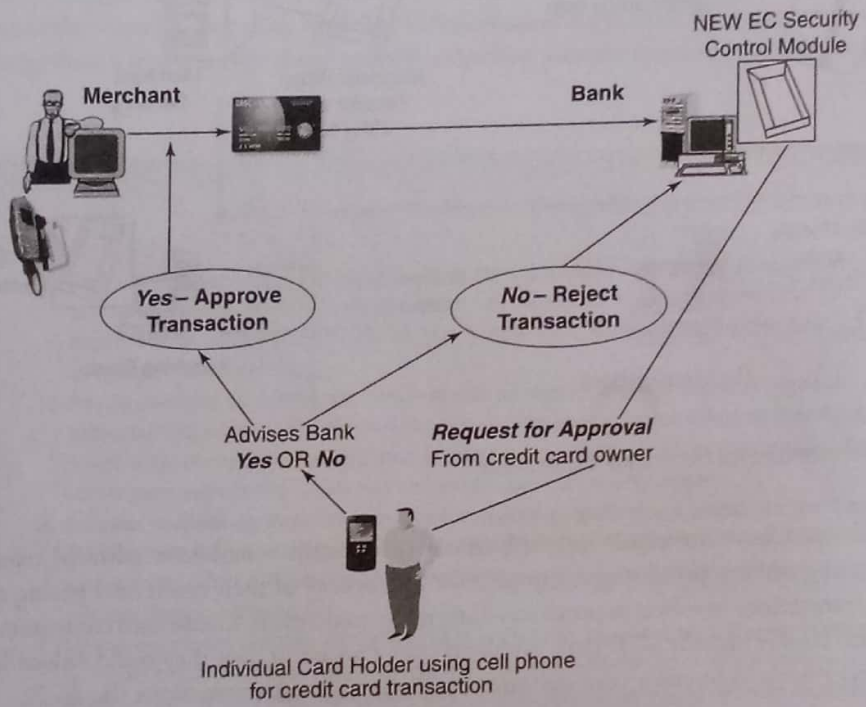


FIGURE 6.5 | CLEW – closed loop environment for wireless.

Courtesy: Alacrity.

As shown in the figure, the basic flow is as follows:

1. Merchant sends a transaction to bank.
2. The bank transmits to cardholder authorization request [*not* short message service (*SMS*)].
3. The cardholder approves or rejects (password protected).
4. The bank/merchant is notified.
5. The credit card transaction is completed.

6.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to the information systems security: on the handheld devices, information is being taken outside of the physically controlled environment, and remote access back to the protected environment is being granted. Perceptions of the organizations to these security challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in Figure 6.6.

As the number of mobile device users increases, two challenges are presented; one at the device level – called 'Micro Challenges' and another one at the organizational level – called 'Macro Challenges'. Of these, some micro challenges are discussed in this section while the macro challenges are discussed in the next section.

Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security, cryptography security, lightweight directory access protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security, etc.* In Sections 6.6 and 6.7, we provide a brief discussion on these security aspects. For most of the discussion here, reference point is Windows mobile development given that the develepors of the Windows OS are on the forefront of the technology in terms of their mobile computing technological

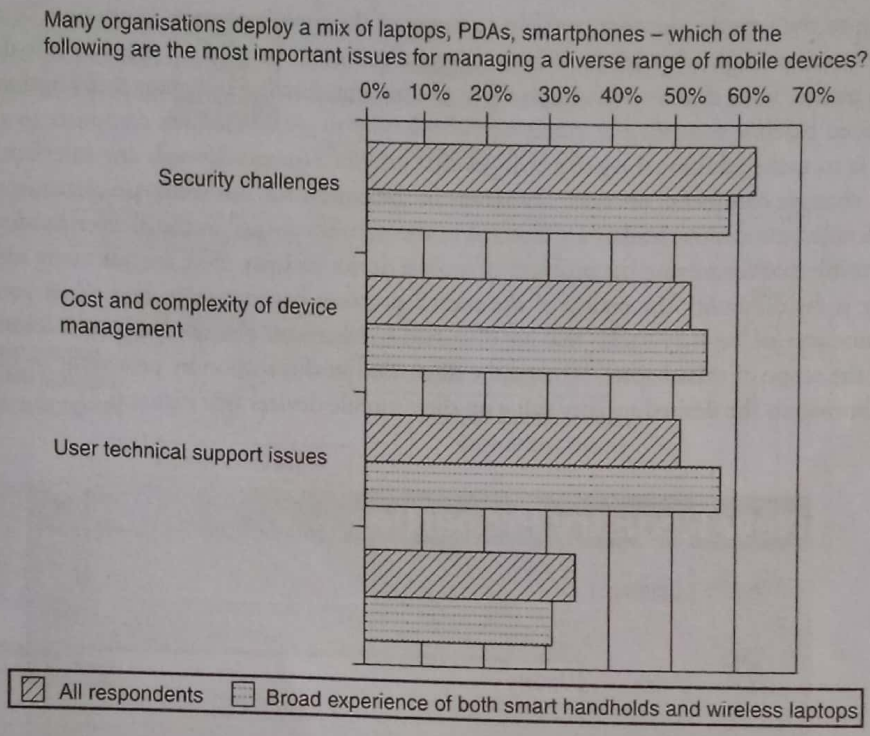


FIGURE 6.6 | Important issues for managing mobile devices.

Courtesy: Mobile Devices and Users – Quocirca Insight Report, June 2005.

initiatives. In view of the discussion in Section 6.4, the ID theft is now becoming a major fraud in credit card business domain; according to the Federal Trade Commission's (FTCs) report on 'Identity Theft' survey (year 2003), participants reported that in the last year they had discovered that their personal information (PI) had been misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care. A full discussion on this is beyond the scope of this chapter.

6.6 Registry Settings for Mobile Devices

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their e-mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within 'group policy'. Group policy is one of the core operations that are performed by Windows Active Directory. As a supporting point, consider the following: within the past two years, Microsoft has doubled the number of group policy settings that it ships with the operating system (OS). There are now nearly 1,700 settings in a standard group policy. The emphasis on most of the group policy settings is security (in the *Further Reading* section a few websites have been quoted where readers can visit for details).

There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against *spyware, viruses, worms, malware* and other malicious codes that run through the networks and the Internet. Microsoft and other companies are trying to develop solutions as fast as they can, but the core problem is still not being

addressed. According to the experts, the core problem to many of the mobile security issues on a Windows platform is that the baseline security is not configured properly. When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every *Control Panel setting* and *group policy* option, they may not get the computer to the desired baseline security. For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional *registry* changes that are not exposed through any interface. There are many ways to get these registry changes completed on every computer in the enterprise, but some are certainly more efficient than the others. For a more detailed discussion, readers are directed to the websites quoted in the *Further Reading* section on this topic.

Naïve users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of 'registry hacks' that are discussed in Microsoft Knowledge Base articles. Further discussion on this topic is beyond the scope of this chapter. We end the discussion in this section by providing an illustration of how some tools allow users to browse to the desired registry value on their mobile devices (see Figure 6.7).

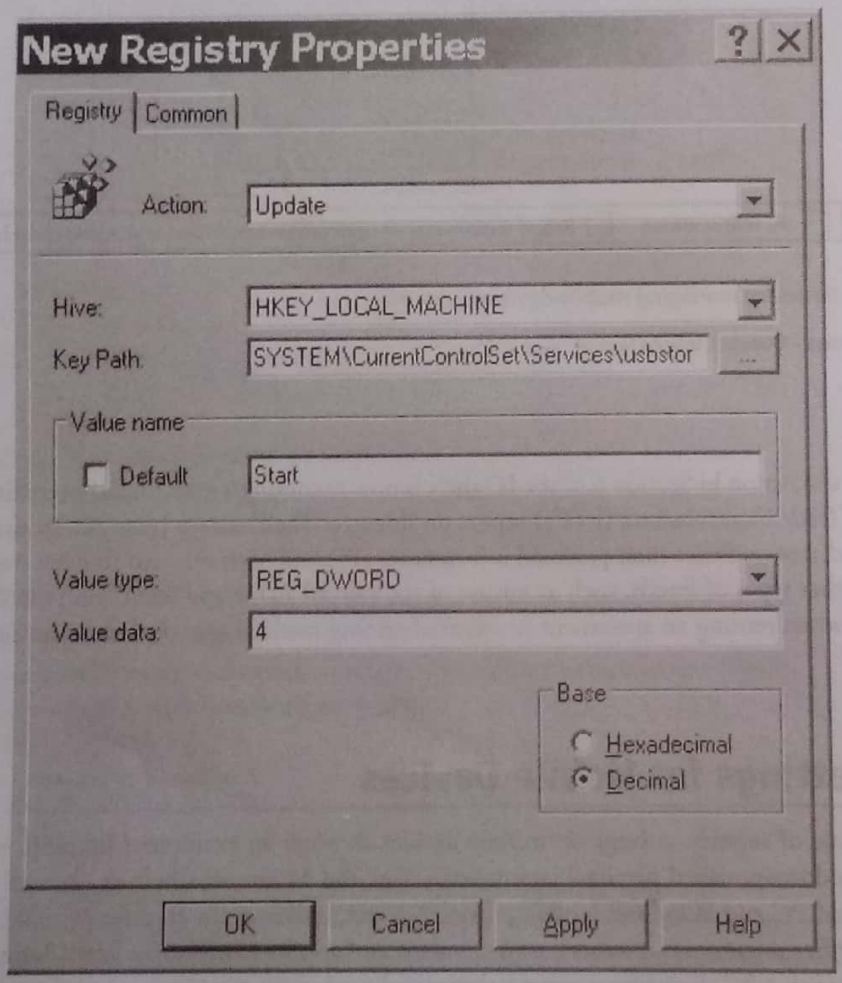


FIGURE 6.7 | Registry value browsing.

6.7 Authentication Service Security

There are two components of security in mobile computing: *security of devices and security in networks.* A secure network access involves the mutual authentication between the device and the base stations or web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No malicious node can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in the security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: *push attacks, pull attacks* and *crash attacks* (see Figures 6.8–6.10).

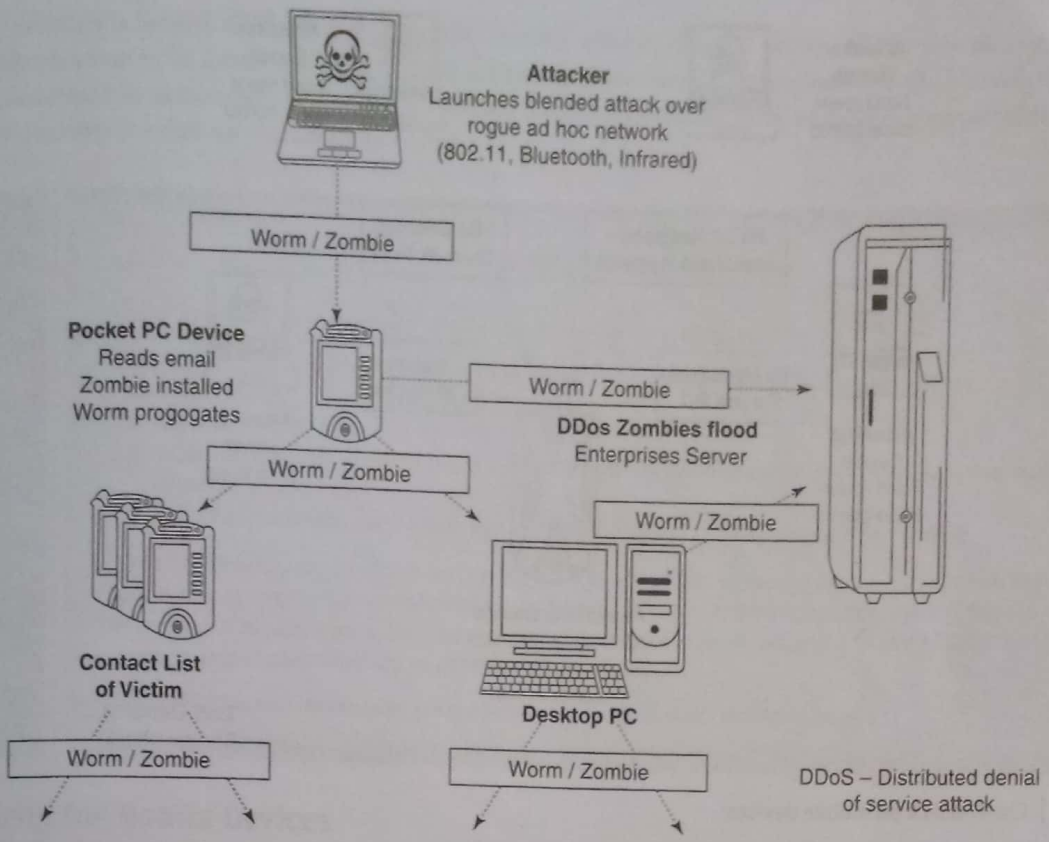


FIGURE 6.8 | Push attack on mobile devices.

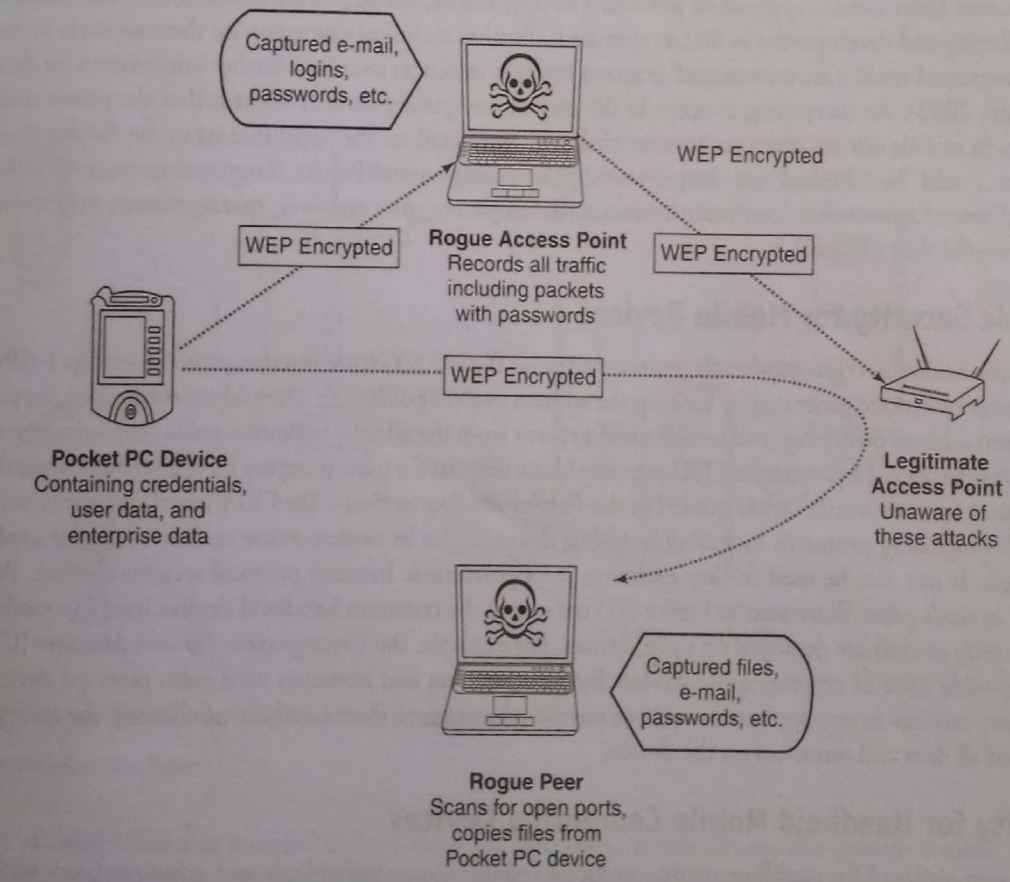


FIGURE 6.9 | Pull attack on mobile devices.

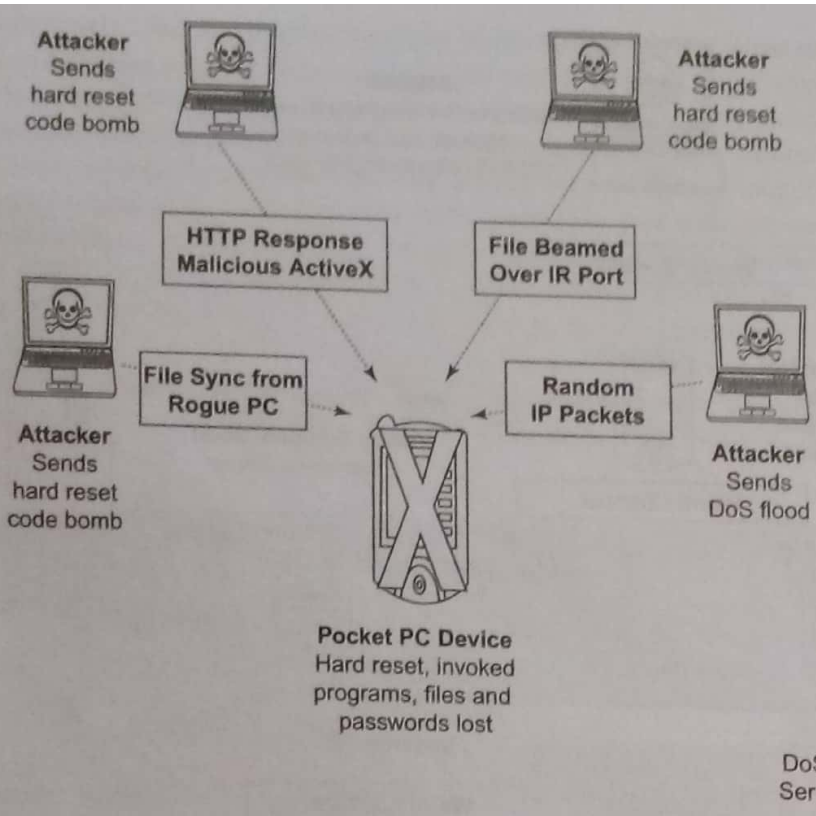


FIGURE 6.10 | Crash attack on mobile devices.

Authentication services security is important given the typical attacks on mobile devices through the wireless networks: *denial of service (DoS) attacks, traffic analysis, eavesdropping, man-in-the-middle attacks* and *session hijacking*. Security measures in this scenario come from *wireless application protocols* (WAPs), use of *virtual private networks* (VPNs), *media access control (MAC) address filtering* and development in 802.xx standards. Further technical discussion on these topics is beyond the scope of this chapter. Interested readers are encouraged to access Internet resources to collect further information on these topics (see Shriraghavan *et al.*, 2003). An interesting concern in the mobile computing security arena is that the power consumption of security measures in mobile devices poses yet another challenge (for detail see the paper quoted in the *Further Reading* section. Other sites that could be checked are http://www.hpl.hp.com/personal/Partha_Ranganathan/papers/2003/2003_lncs_escale.pdf; http://www.forum.nokia.com/main/resources/development_process/ower_management/; http://www.cs.umass.edu/~nilanb/papers/Mobisys05.pdf.).

Cryptographic Security for Mobile Devices

There is a technique known as *cryptographically generated addresses* (CGA). CGA are Internet protocol version 6 (IPv6) addresses where up to 64 address bits are generated by hashing the address owner's public key. The address owner uses the corresponding private key to assert address ownership and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices (see one source article quoted in the *Further Reading* section). The CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in *context-aware mobile computing applications*) and mobility protocols. It can also be used for key exchange in opportunistic Internet protocol security (IPSec). Palms (devices that can be held in one's palm, illustrated in Figure 6.1) are one of the common handheld devices used in mobile computing. *Cryptographic security controls* are deployed on these devices. For example, the *Cryptographic Provider Manager* (CPM) in Palm OS 5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

LDAP Security for Handheld Mobile Computing Devices

LDAP is a software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet. In a network, a directory tells you where in

the network an entity is located. LDAP is a 'lightweight' (smaller amount of code) version of *directory access protocol* (DAP). LDAP is lighter because in its initial version it did not include security features. It originated at the University of Michigan and has been endorsed by at least 40 companies. Centralized directories such as LDAP make revoking permissions quick and easy. Box 6.3 describes the directory structure of LDAP.

BOX 6.3

LDAP Directory Structure

An LDAP directory is organized in a simple 'tree' hierarchy consisting of the following levels:

1. the *Root Directory* (the starting place or the source of the tree) which branches out to
2. *countries*, each of which branches out to
3. *organizations*, each of which branches out to
4. *organizational units* (geographies/divisions, departments and so forth), each of which further branches out to (includes an entry for)
5. *individuals* (which, in turn, include people, files and shared IT resources such as printers).

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a *directory systems agent* (DSA). An LDAP server that received a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user.

Courtesy: http://searchmobilecomputing.techtarget.com/sDefinition/0, sid40_gci214076,00.html.

RAS Security for Mobile Devices

RAS is an important consideration for protecting the business-sensitive data that may reside on the employees' mobile devices. In terms of InfoSec, mobile devices are sensitive (Figure 6.11 illustrates how access to an organization's sensitive data can happen through mobile handheld devices carried by employees).

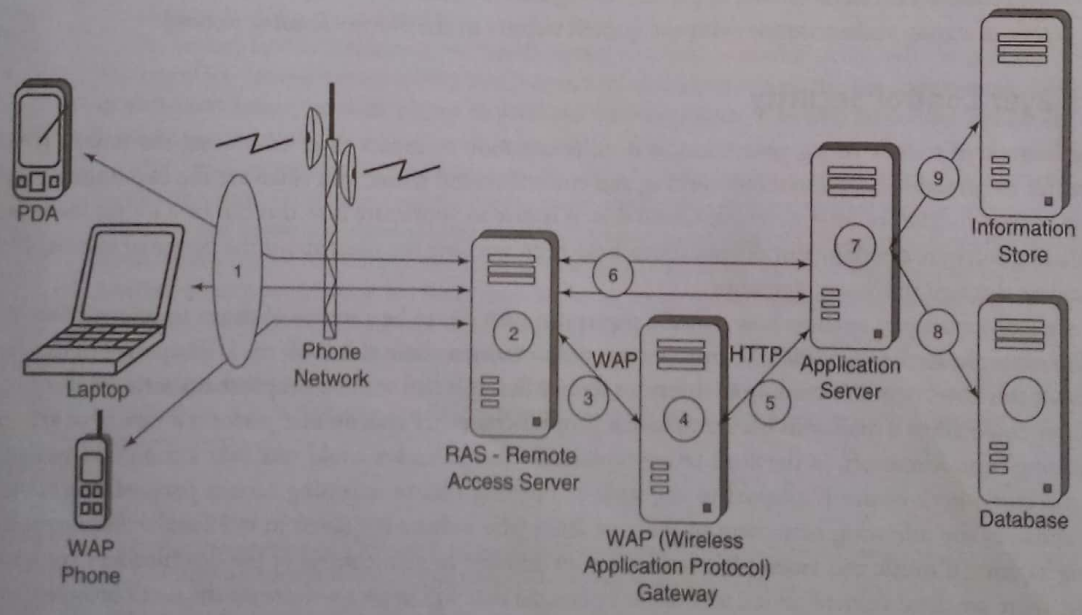


FIGURE 6.11 | Communication from mobile client to organization information store.

Courtesy: Ericsson Security White Paper.

In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (*impersonating* or *masquerading*) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

Another threat comes from the practice of *port scanning*. First, crackers use a domain name system (DNS) server to locate the *IP address* of a connected computer (either the mobile device itself or a gateway server to which it connects). A *domain* is a collection of sites that are related in some sense. Then they scan the ports on this known IP address, working their way through its transmission control protocol (TCP)/user datagram protocol (UDP) stack to see what communication ports are unprotected by firewalls. For instance, *file transfer protocol* (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by hackers (Box 6.4).

BOX 6.4

RAS System Security for Mobile Device Clients

The security of an RAS system can be broken down into three areas:

1. the security of the RAS server;
2. the security of the RAS client;
3. the security of data transmission.

Whereas the desired level of security of the RAS server can be controlled through implementation of local security guidelines, the RAS client (e.g., a mobile handheld device) is typically not under the complete control of the IT personnel who is responsible for the local area network (LAN). The security of the data transmission media is generally completely out of their control. For this reason, protection of communications between the client and the server must be secured by additional means.

See the article quoted in the *Further Reading* section for further details.

Protecting against port scanning requires software that traps unauthorized incoming *packets*, thereby preventing a mobile device from revealing its existence and ID. A *personal firewall* on a pocket PC or smart phone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement *strong authentication keys* will provide an additional protection (for more technical details of strong authentication, visit the quoted website in the *Further Reading* section).

Media Player Control Security

Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile handheld devices as a means for information access, remote working and entertainment! Music and video are the two important aspects in the day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for security breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the 'music gateways'.

There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft corporation warned about this (visit the URL quoted in the *Further Reading* section about this news item). According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people's computer systems and perform a variety of actions. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network. As another example, consider the following news item of the year 2004 (the website is quoted in the *Further Reading* section): corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer. With this happening, there are three vulnerabilities: files could be created that will open a website on the user's browser (which, e.g., the user could be accessing from his/her handheld device) from where remote JavaScript can be operated, files could be created which allow the attacker to download and use the code on a user's machine, or media files can be created that will create buffer overrun errors.

In Section 6.6 we discussed registry settings in connection with the mobile devices' security. This topic becomes important in the context of the current section too. Registry of a computing device is always an important concept; the registry stores information necessary to configure the system for applications and hardware devices. It also contains information that the OS continually references during an operation. In the registry, some keys control the behavior of the Windows Media Player

control. Microsoft, through its developer network MSDN, describes details of registry value settings on the mobile devices (interested readers can visit some such websites quoted in the *Further Reading* section). With the increase in our mobile workforce and the resulting increase in the number of mobile computing handheld devices used by the young employees of most IT and software organizations, it would be quite common to expect such security attacks and hence one should be ready for security measures.

Networking API Security for Mobile Computing Applications

With the advent of electronic commerce (e-commerce) and its further off-shoot into *m-commerce*, online payments are becoming a common phenomenon with the *payment gateways* accessed remotely and possibly wirelessly. Further, with the advent of *web services* and their use in mobile computing applications (author's paper in this area is quoted in the *Further Reading* section), the API becomes an important consideration. Operators and handset developers are increasingly motivated to create even more advanced features for mobile phones, such as one that would enable a phone to double as a credit card and a digital television (TV) player, but they have to ensure that the users and devices are adequately protected from the external threats.

Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways (see Box 6.5).

BOX 6.5

TrustZone Technology for Mobile Devices: Toward Security of m-Commerce Applications

About two years back, *Trusted Logic Security Module* was announced for *Microsoft Windows CE 5.0*. With this, developers of Windows CE 5.0 can use Trusted Logic software to increase *electronic transaction security* in ARM-powered(R) devices, which is very pertinent in the m-commerce paradigm.

The Windows CE 5.0 evaluation version of the security module, coupled with the ARM TrustZone technology, provides consumers with a more *secure environment for electronic transactions* such as *m-banking, electronic commerce (e-commerce)* and digital rights management (DRM). This security can be designed into ARM-powered consumer devices such as *mobile phones, payment terminals* and *set-top boxes*.

The security module implements the TrustZone APIs to enable smooth evolution and compatibility with future versions of the software running on ARM TrustZone technology-enabled processors. The software is part of a portfolio of embedded security products offered by ARM and developed under a recently announced agreement between Trusted Logic and ARM.

ARM TrustZone architecture extensions build security into the processor itself while TrustZone software provides trusted foundation software, protected by the hardware, enabling OS providers, handset vendors and silicon designers to expand and develop their own security solutions on top of an interoperable framework. Currently, security-aware applications must be rewritten for every security platform they run on. However, the new TrustZone Software API provides a standard interface for these applications to be partitioned and to communicate with a secure-side component independent of the actual system implementation.

According to the experts, m-commerce applications can now target multiple security platforms and speed up the development. Industry analysts say that this is a technical collaboration between Microsoft and ARM. This is being considered as a good step toward making mobile devices more secure and is critical to the success of next-generation mobile applications.

Courtesy:

1. http://www.trusted-logic.com.
2. http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/09-07-2005/0004101444&EDATE.
3. http://www.finanznachrichten.de/nachrichten-2004-09/artikel-3904215.asp.

Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices). Technological developments such as these provide the ability to significantly improve the security of a wide range of consumer as well as mobile devices. Providing a common software framework and APIs will become an important enabler of new and higher value services.

6.8 Mobile Devices: Security Implications for Organizations

Managing Diversity and Proliferation of Handheld Devices

In the previous sections, we talked about the micro-issues of purely technical nature in mobile device security. In this section, we focus on the macro-issues at the organizational level. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, while others will place more value on cost and convenience. Whatever approaches an organization chooses, it is important that the policy-making effort starts with the commitment from a Chief Executive Officer (CEO), president or director who takes security seriously and communicates that throughout an organization. The best security technology features are worthless if there is no organization policy or automated enforcement to ensure that they are actually used. In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures.

Security is always a primary concern; even then, at times, there is still some short-sightedness. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether the devices have been provided by the organization or not. In addition (recall the micro-level technical issues discussed in the previous section), close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices which belong to the company should be returned to the IT department and, at the very least, deactivated and cleansed.

In addition, employees should be encouraged to register with the IT department any devices they provide for themselves, so that access can be provisioned in a controlled manner, and de-provisioned appropriately when the employee leaves. Standards such as BS 7799/ International Organization for Standardization (ISO) 17799 expect compliance to security best practices under *asset management* (Box 6.6).

BOX 6.6

ISO 17799 – Main Clauses (Changes from 2000 to 2005 Release)

2005	2000
1. Security policy	1. Security policy
2. Organizing InfoSec	2. Organizational security
3. Asset management	3. Asset classification and control
4. Human resource security	4. Personnel security
5. Physical and environmental security	5. Physical and environmental security
6. Communications and operations management	6. Communications and operations management
7. Access control	7. Access control
8. Information systems acquisition, development and maintenance	8. Systems development and maintenance
9. InfoSec and incident management	9. —
10. Business continuity management	10. Business continuity management
11. Compliance	11. Compliance

Courtesy: IS Control Journal, Vol. 1, 2006 – an Information Systems Audit and Control Association (ISACA) Publication (www.isaca.com).

We have already mentioned about user 'perceptions' in security matters. Here is an interesting illustration on this point; unlike laptops, which owing to their cost are generally provided as a corporate item requiring significant sign-off and approvals, many handhelds can be squeezed under approval limits or be purchased by the individual. Their usage often falls outside the range of the IT department's scope of control.

Thus, another factor in security complications with mobile devices is their falling cost. Until a few years ago, mobile devices were considered an office supply item instead of a powerful computing platform. Early handhelds were *expensive*

and *specialized*, so they were deployed only for specific applications, but more general-purpose models are now available at a relatively low cost, often bundled with a tariff for wireless connection. So, many organizations did not have policies concerning the usage of mobile/wireless devices at work/connected with work. Nowadays, because modern handheld devices for mobile computing are, at times, good productivity tools, they cannot be precluded from use by employees, contractors and other business entities. Given this, it is important for the device management teams to also include user awareness education; thus, they get encouraged to take some personal responsibility for the physical security of their devices, as many IT managers have learned from bitter experience.

Threats Through Lost and Stolen Devices

This is a new emerging issue for InfoSec. Often mobile handheld devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. A report (see the URL quoted in the *Further Reading* section) based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last six-month period. Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices (for details on the numbers, see the RIM reports quoted in the *Further Reading* section). See Box 6.7 for some interesting facts on lost mobile devices.

BOX 6.7

Getting Lost!!

Cities and countries in which drivers were surveyed were Chicago; Copenhagen, Denmark; Helsinki, Finland; London; Munich, Germany; Oslo, Norway; Paris; Stockholm, Sweden and Sydney, Australia.

1. Pointsec Mobile Technologies, Inc. has discovered where lost electronic devices go: they wind up in the back seats of taxis all around the world!!
2. A survey of 935 cabbies in nine countries turned up 85 notebook computers, 227 PDAs and 2,238 cell phones lost in cabs in the last six months.
3. As per Gartner 2002 report, nearly 250,000 handheld devices were left behind in US airports in 2002, and of those, only about 30% were traced back and returned to their owners.
4. Copenhagen appears to have the most forgetful cell phone users, with 719 phones left behind in 100 cabs in a six-month period. Chicago cab riders left behind 387 in the same period. Ninety-seven PDAs were reported lost in Chicago, as were 20 notebooks. London cabbies reported 23 laptops left behind.
5. As per Gartner 2004 study, a company with 5,000 or more employees could save USD 300,000–500,000 annually by tagging, tracking and recovering mobile phones and PDAs.

Courtesy: http://www.gcn.com/online/vol1_no1/34896-1.html.

The security threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the handheld device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity as most of the times, the mobile handheld devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and potentially very little security, making them a weak link and a major headache for security administrators. Even if these lost devices are personal, the issue is no less serious given the resulting privacy exposures! Gartner Group had predicted that by 2003 there will be over one billion mobile devices in use globally. Going by the sales figures quoted in annual reports published by Research in Mobile, this is true (RIM reports quoted in the *Further Reading* section). This shows that the popularity of mobile devices is increasing at a rapid rate, but people have not been educated about the importance of securing them. The picture is indeed scary; mobile users are in an even worse position now because they are far more reliant on their mobile devices to store large amounts of sensitive information with very few concerned about backing it up or protecting it.

Protecting Data on Lost Devices

Given the above discussion, readers can appreciate the importance of data protection especially when it resides on a mobile handheld device. At an individual level, employees need to worry about this. There are two reasons why InfoSec needs to address this issue: data that are persistently stored on the device and always-running applications. For protecting data that are

stored persistently on a device, there are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device: encrypting sensitive data and encrypting the entire file system (this may be useful when using data outside of a database, such as in a spreadsheet). Data that are stored on hard disks, in persistent memory or on removable flash cards (whether they are in or out of the device) should be protected. There are many third-party solutions/tools available to protect data on the lost devices in several ways, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device, or create a database action to delete the data on a user's device using a suitable tool.

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

Educating the Laptop Users

Often, it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and spyware. This is because the software assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options. A number of surveys conducted worldwide support this (see the *Further Reading* section for sources of these surveys). Some are described below.

According to year 2004 finding, through one survey, some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and download illegal music files and movies. As per one survey of 500 European business laptop users, malicious code, such as spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.

The result from a survey quoted in Figure 6.12 further supports this point on InfoSec threats from corporate laptop users. However, despite the growth in corporate security risks, resulting from mobile working, the tone of most of the security-awareness surveys shows that only half of the companies have tools in place to manage Internet access on laptops, with only one-quarter of businesses physically enforcing these policies. An important point to be taken is that the policies and procedures put in place for laptop support have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise. This shows how much role 'perception' plays in terms of most people perceiving laptops as greater culprits than other innocuous-looking mobile handheld devices.

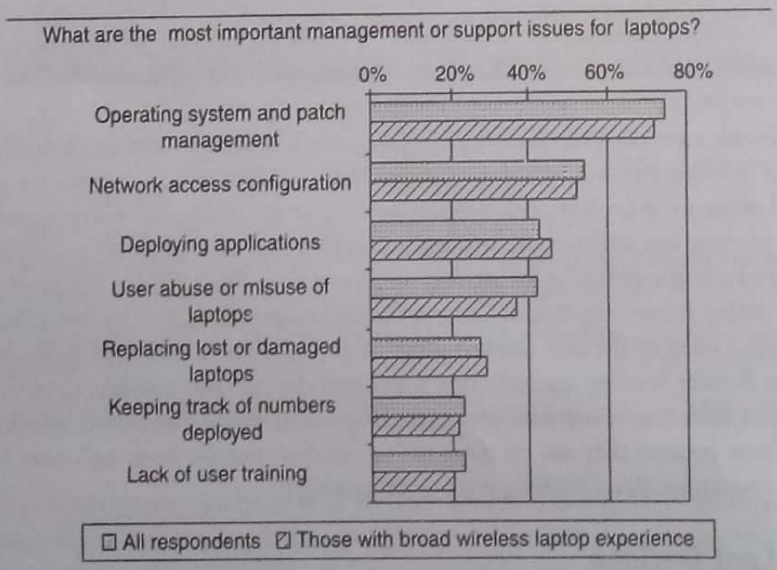


FIGURE 6.12 | Most important management or support issues for laptops.

Courtesy: Mobile devices and users – June 2005 report of Quocirca.

6.9 Organizational Measures for Handling Mobile Devices Related Security Issues

So far, we have discussed micro- and macro-level security issues with mobile devices used for mobile computing purposes and what individuals can do to protect their personal data on mobile devices. In this section, we discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

Encrypting Organizational Databases

Critical and sensitive data reside on databases say, applications such as customer relationship management (CRM) that utilize patterns discovered through *data warehousing* and *data mining* (DM) techniques and with the advances in technology, access to these data is not impossible through handheld devices. It is clear that to protect the organizations' data loss, such databases need encryption. We mention here two algorithms that are typically used to implement strong encryption of database files: Rijndael (pronounced rain-dahl or Rhine-doll) and a block encryption algorithm chosen as the new Advanced Encryption Standard (AES) for block ciphers by the National Institute of Standards and Technology (NIST). Readers are urged to visit the Rijndael-related websites quoted in the *Further Reading* section. The other algorithm used to implement strong encryption of database files is Multi-Dimensional Space Rotation - the MDSR algorithm, developed by Casio.

The term 'strong encryption' is used here to describe these technologies, in contrast to the simple encryption. *Strong encryption* means that it is much harder to break, but it also has a significant impact on performance. Database file encryption technology, using either the AES or the MDSR algorithms, makes the database file inoperable without the key (password). Encrypting the database scrambles the information contained in the main database file: all temporary files and all transaction log files, so that it cannot be deciphered by looking at the files using a disk utility. There is a performance impact for using strong encryption. A weaker form of encryption is also available that has negligible performance impact.

When using strong encryption, it is important *not* to store the key on the mobile device: this is equivalent to leaving a key in a locked door. However, if you lose the key, your data are completely inaccessible. The key is case sensitive and must be entered correctly to access your database. The key is required whenever you want to start the database or you want to use a utility on your database. For greater security there is an option available that instructs the database server to display a dialog box where the user can enter the encryption key. This option is necessary because the encryption key should not be entered on the machine in clear text. To protect the scenario of information attack/stealing through the mobile devices connecting to corporate databases, additional security measures are possible through enforcing a self-destruct policy that is controlled from the server. When a device that is identified as lost or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

Including Mobile Devices in Security Strategy

The discussion so far makes a strong business case – in recognition of the fact that our mobile workforce is on the rise, organizational IT departments will have to take the accountability for security threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection being used. Their concerns are no longer viable. There are technologies available to properly secure mobile devices. These should be good enough for most organizations. Corporate IT departments just need to do their homework. For example, there are ways to make devices lock or destroy the lost data by sending the machine a special message. Also, some mobile devices have high-powered processors that will support 128-bit encryption. Although mobile devices do pose unique challenges from a security prospective, there are some general steps that the users can take to address them, such as integrating security programs for mobile and wireless systems into the overall security blueprint. A few things that enterprises can use are:

1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
3. Develop a system of more frequent and thorough security audits for mobile devices.

4. Incorporate security awareness into your mobile training and support programs, so that everyone understands just how important an issue security is within a company's overall IT strategy.
5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

In the next section, our focus is on security policies relating to mobile devices.

6.10 Organizational Security Policies and Measures in Mobile Computing Era

Importance of Security Policies Relating to Mobile Computing Devices

Proliferation of handheld devices used makes the security issue graver than what we would tend to think. People (especially, the youth) have grown so used to their handhelds that they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their handheld devices (we have already discussed the threats through media player when we talked about micro-level technical issues for InfoSec threats through these devices). Think about where you keep your credit card and bank account numbers, passwords and confidential e-mails. What about strategic information about your organization? Merger or takeover plans? And also may be the information that could impact stock values? Imagine the business impact if an employee's universal serial bus (USB) pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information. Not only would this be a public relations (PR) disaster, but it could also violate laws and regulations. Consider the potential legal troubles for a public company whose sales reports, employee records or expansion plans fall into wrong hands.

When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure. This sort of policy can be difficult to enforce, but, in conjunction with good user education, it can be reasonably effective. Information classification and handling policy should clearly define what sorts of data may be stored on mobile devices. In the absence of other controls, simply not storing confidential data on at-risk platforms will mitigate the risk of theft or loss.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the company, industry and regulatory environment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques (retinal scans, iris scans, etc.; this topic will be discussed in Chapter 11) are increasingly being used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data-syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory (we have stressed on this point in the section called 'Managing Diversity and Proliferation of Hand-held Devices' as explained in Section 6.8) so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing, or patch management with the centralized inventory database.
7. Label the devices and register them with a suitable service which helps return recovered devices to the owners.

8. Establish procedures to disable remote access for any mobile devices reported as lost or stolen. Many devices allow the users to store usernames and passwords for website portals, which could allow a thief to access even more information than on the device itself.
9. Remove data from computing devices that are not in use or before re-assigning those devices to new owners (in case of company-provided mobile devices to employees). This is to preclude incidents through which people obtain 'old' computing devices that still had confidential company data.
10. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Handheld Devices

The first step in securing mobile devices is creating company policies that address the unique issues these devices raise. Such questions include what an employee should do if a device is lost or stolen. We have talked about this in the section called 'Protecting Data on Lost Devices' (Section 6.8).

There are many ways to handle the matter of creating policy for mobile devices. One way is creating a distinct mobile computing policy. Another way is including such devices under existing policy. There are also approaches in between, where mobile devices fall under both existing general policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices (such as what to do if they are lost or stolen) but more general usage issues fall under general IT policies. As a part of this approach, the 'acceptable use' policy for other technologies is extended to the mobile devices. There may not be a need for separate policies for wireless, LAN, wide area network (WAN), etc. because a properly written network policy can cover all connections to the company data, including mobile and wireless.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time that they will need to modify their policies to match the challenges posed by different kinds of mobile handheld devices. For example, wireless devices pose different challenges than non-wireless devices. Also, employees who use mobile devices more than 20% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs.

It is never too early to start planning for mobile devices, even if a company, at a given point of time, cannot afford creating any special security policies to mitigate the threats posed by mobile computing devices to InfoSec. It is, after all, an issue of new technology adoption for many organizations. By contemplating its uses, companies may think of ways they can use it and, perhaps just as important, how their competitors will use it.

6.11 Laptops

As the price of computing technology is steadily decreasing, devices such as the laptops have become more common in use. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable. Wireless capability in these devices has also raised security concerns owing to the information being transmitted over ether, which makes it hard to detect. In this section, we provide an elaborate discussion as to what measures the organizations can take in the face of information systems security threat brought by the wide-spreading use of laptops.

According to the computer security industry and insurance company statistics, thefts of laptops have always been a major issue. Criminals are targeting laptop systems that are expensive as they could fetch them a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information which could be sensitive. Such information can be misused if found by a malicious user. It is a common belief of senior executives in an organization to think that the information stored on their laptops is only useful for them and would not be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. However, this is not true. The following section provides some countermeasures against the theft of laptops, thereby avoiding InfoSec exposures.

Physical Security Countermeasures

1. **Cables and hardwired locks:** Securing with cables and locks, specially designed for laptops, is the most cost-efficient and ideal solution to safeguard any mobile device. Kensington cables are one of the most popular brands in laptop security cables (see Figures 6.13 and 6.14). These cables are made of aircraft-grade steel and Kevlar brand fibber, thus

FIGURE 6.13 | Cable lock for laptops.

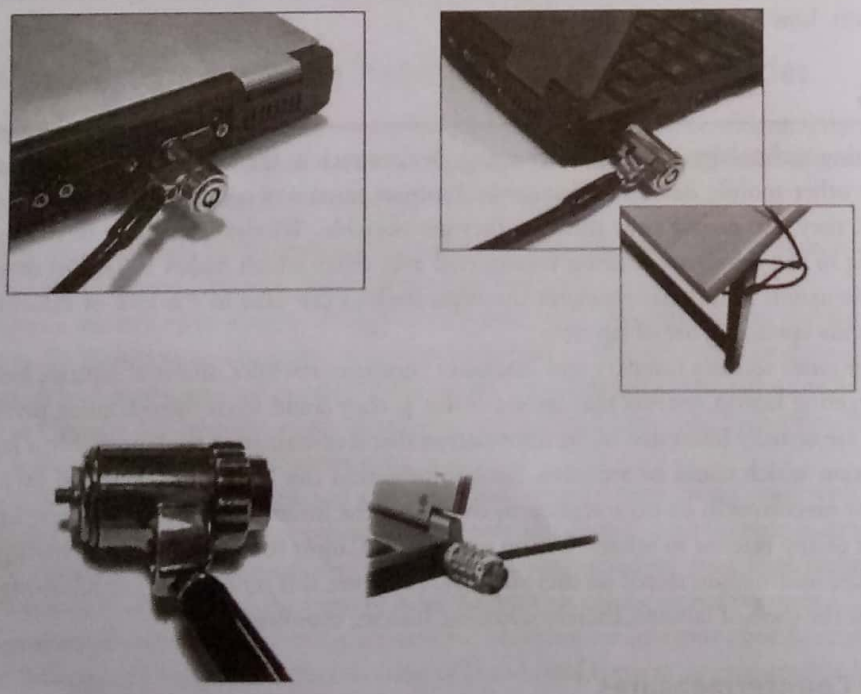


FIGURE 6.14 | Closer view of cable locks for laptops.

making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms. However, the downside of the security cables lies in the fact that one can easily remove detachable bays like compact disk read-only memory (CD-ROM) bay, Personal Computer Memory Card Industry Association (PCMCIA) cards (see the URL in the *Further Reading* section), hard disk drive (HDD) bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object which is not fixed or is weak enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was attached to.

2. **Laptop safes:** Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in case of laptops protected by security cables.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once activated, these devices can be used to track missing laptops in crowded places. Also owing to their loud nature they help in deterring thieves. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device which communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. Also available are security PCMCIA cards that act as a motion detector, an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries which keep them powered on even when the system is shutdown. Figure 6.15 shows some laptop alarm systems with sensors.

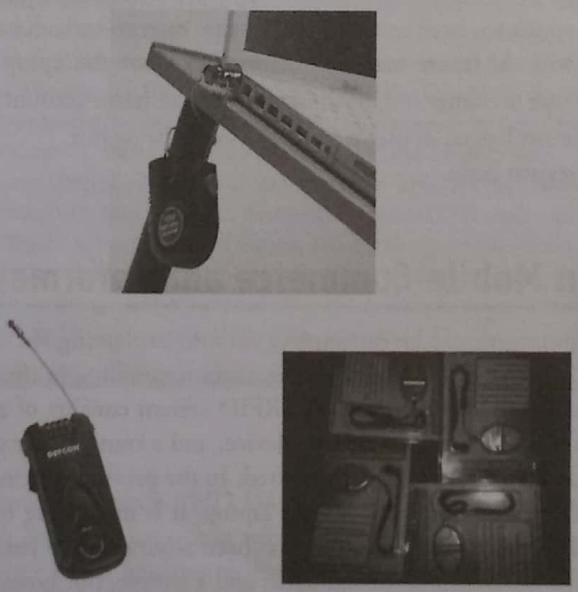


FIGURE 6.15 | Laptop alarm systems with sensors.

4. **Warning labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number which is stored in a universal database for verification, which in turn makes the resale of stolen laptops a difficult process.
5. **Other measures for protecting laptops:**
   - Engraving the laptop with personal details;
   - keeping the laptop close to oneself wherever possible;
   - carrying the laptop in a different and unobvious bag making it unobvious to potential thieves;

- making the employee understand about the responsibility of the laptop and also about the sensitivity of the information contained in the laptop;
- making a copy of the purchase receipt, laptop serial number and the description of the laptop;
- installing encryption software to protect information stored on the laptop;
- using personal firewall software to block unwanted access and intrusion;
- updating the antivirus software regularly;
- tight office security using security guards and securing the laptop by locking it down in lockers when not in use;
- never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti-theft device;
- disabling infrared (IR) ports and wireless cards and removing PCMCIA cards when not in use.

So far, we have discussed protection of corporate laptops in terms of physical access control. However, information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical access controls are as follows:

1. Protecting from malicious programs/hackers/social engineering;
2. avoiding weak passwords/open access;
3. monitoring application security and scanning for vulnerabilities;
4. ensuring that unencrypted data/unprotected file systems do not pose threats;
5. proper handling of removable drives/storage mediums/unnecessary ports;
6. password protection through appropriate passwords rules and use of strong passwords;
7. locking down unwanted ports/devices;
8. regularly installing security patches and updates;
9. installing antivirus software/firewalls/intrusion detection systems (IDSs);
10. encrypting critical file systems;
11. other countermeasures:
    - choosing a secure OS which has been tested for quite some time and which has a high security incorporated into it,
    - registering the laptop with the laptop manufacturer to track down the laptop in case of theft,
    - disabling unnecessary user accounts and renaming the administrator account,
    - disabling display of the last logged in username in the login dialog box,
    - backing up data on a regular basis.

6.12 Use of RFID in Mobile Commerce and Information Asset Protection

The discussion on mobile computing would be incomplete without explaining the use of radio frequency identification (RFID) technology. With RFID, the electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the RF and transfer the information to a processing device, and a transponder or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted. In the previous section, we showed some pictures of cable locks, alarm systems, etc. for the physical security of your laptop; it is interesting to note that with RFID tag, you can track your stolen/lost laptop. Although RFID technology has been around for 50 years, it was not considered practical for wide adoption until recently. The development of standards and a simple, but powerful, network model has helped this technology take hold. Additionally, tags are becoming less expensive and smaller, making it more attractive for businesses to implement.

RFID systems can be used just about anywhere, from clothing tags to missiles to pet tags to food – anywhere that a unique identification system is needed. The tag can carry information as simple as a pet owner's name and address or the cleaning instruction on a sweater to as complex instructions as on how to assemble a car. Some auto manufacturers use RFID systems to move cars through an assembly line. At each successive stage of production, the RFID tag tells the computers what the next step of automated assembly is. Readers may be familiar with the bar code technology through their own shopping experience wherein the universal product code of an item purchased is picked up by the scanner at a POS terminal and its price from the store inventory is picked up by the sales clerk. One of the key differences between an RFID and a bar code technology is that the RFID eliminates the need for line-of-sight reading something that bar coding

depends on. Also, RFID scanning can be done at greater distances than bar code scanning. High-frequency RFID systems (850–950 MHz and 2.4–2.5 GHz) offer transmission ranges of more than 90 ft, although wavelengths in the 2.4 GHz range are absorbed by water (the human body) and therefore have limitations. RFID is also called dedicated short-range communication (DSRC).

With RFID, one area of technology innovation in which savvy companies are investing is *Silent Commerce*. This refers to business benefits derived from new types of applications that can track and monitor objects remotely, without people being involved. Silent Commerce covers all business solutions enabled by tagging, tracking, sensing and other technologies, including RFID, which make everyday objects intelligent and interactive. When combined with continuous and pervasive Internet connectivity, they form a new infrastructure that enables companies to collect data and deliver services without human interaction (Box 6.8).

BOX 6.8

RFID-based Physical Protection for Laptops

The 2005 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Annual Computer Crime and Security Survey was responded to by over 900 IT practitioners who divulged that the cost to organizations related to the loss or theft of proprietary data doubled over the last year to USD 356,000 per incident. The New York Stock Exchange (NYSE) has now instituted a rule that all NYSE-listed company's 'employees, officers and directors should maintain the confidentiality of information entrusted to them by the company or its customers'.

The trend toward more mandates is clear. Under the Sarbanes–Oxley Act ('SOX') in Sections 404 and 302, the protection of corporate assets is the responsibility of the executive office where the management is to establish and maintain 'an adequate internal control structure and procedures for financial reporting'. What is the exposure of not protecting laptops if their loss substantially impacts the value of corporate assets? The courts require that reasonable steps be taken to protect information in order for that information to qualify as confidential information such as a trade secret in the event of a dispute.

The profile of a laptop thief is also very different from the common perception. Most people think the thefts happen by burglars at night or by cleaning personnel. To combat such occurrences, early attempts centered on cabling laptops to the desks. However, the FBI's statistics show that 75% of the thefts are perpetrated by fellow employees or by the employees themselves; hence, the cables offered no protection as they simply get cut by an innocent-looking coworker. Additionally, cables impact a laptop's ability to be mobile as intended.

This financially and competitively costly problem requires what the physical security industry calls 'automatic identification and protection'. One needs the flexibility to move about a facility with your authorized laptop, or even leave the facility with your authorized laptop without security unreasonably impacting you or being 'intrusive'. RFID systems offer this option. 'Active' RFID tags have embedded batteries to enable the tag to transmit autonomously, either by beaconing or by being automatically activated at a doorway or virtual 'control point'. This means that assets can be automatically identified, tracked and, therefore, protected.

Further development is what is known as mobile RFID (M-RFID) – M-RFID can be defined as service that provides information on objects equipped with an RFID tag over a telecommunication (TC) network. The reader is installed in a mobile device such as a mobile phone or a PDA. This completely new approach is different from current implementations of ordinary RFID: now the readers are mobile and the tags are fixed, instead of the other way around. M-RFID has some major and obvious advantages over RFID: no wires to fixed readers are needed anymore and several mobile readers, instead of dozens of fixed readers, are enough to cover a whole area.

6.13 Wearable Devices and Security Threats

IoT (Internet of Things) integrates a number of digital technologies across the technology landscape. MIT professor Aaron Fleisher is considered as the visionary in the domain, given his writing way back 1961 wherein he wrote 'The Influence of Technology on Urban Forms' (in the reference section at the end, a link is mentioned to this). Now, the new breed of devices

called 'wearable devices' is on the technology horizon; in fact some of them are already in use (e.g., the device called 'fitbit' that is worn on the wrist). A point to note is that the connectivity of mobile hand-held devices has gone far beyond just the wireless communication technology and it is now embracing the IoT technology. It is in this context, that we discuss the security threats to wearable devices in this section.

Refer to Chapter 10 – The Internet of Things (IoT) and Smart Cities: Security and Privacy Challenge.

It is to be noted that due to the advances of IoT (see Chapter 10) these devices can 'communicate' with other digital devices and that raises a few concerns, including security threats as well as privacy concerns (the fundamentals of privacy are explained in Chapter 27).

In the past 20 years Internet has invaded our planet; it is now almost omnipresent. Talking in terms of 'half-life', it took only a decade for smartphones to reach that ubiquity. Noting this amazing rate of technology dissemination, the question is 'will wearables spread at an even faster rate?'. Cisco predicts more than 600 million wearable devices in use by 2020. Gartner Research, a well-known research organization, has predicted that by year 2017 the frequency of mobile apps download will be 268 billion times and that it is expected to generate revenue of $77 billion. It further predicts that in year 2017, 50% percent of all application interactions will come not from smartphones, but from 'wearable devices'. In fact, forward-looking organizations are considering 'wearables' as an opportunity for mobile technology to drive greater efficiency, to enhance communication and to improve workflow. Thus, the writing on the wall is clear; there is going to be an explosion in wearable applications.

So, let us understand what wearable devices are (see Figure 6.16); you may already be aware with some of them – for example the 'smart wrist watches' that can monitor your heart rate, your pace of walking, etc. and that is only the rudimentary part of the wearables to come in the future. *Wearable gadgets* and *wearable technology* are the two terms often used interchangeably - this

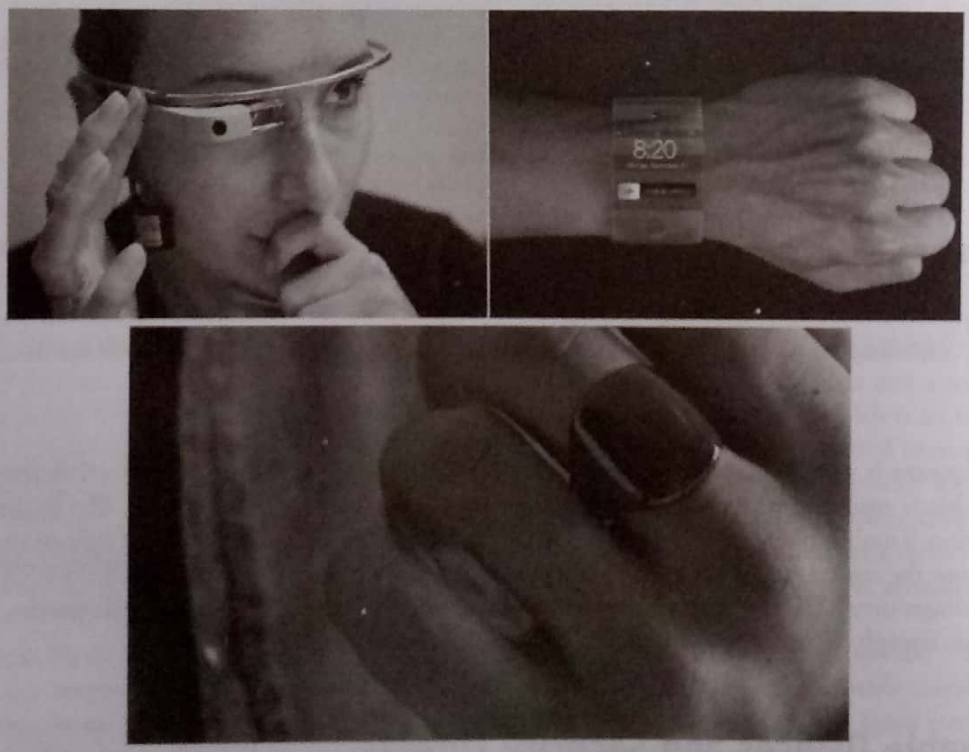


FIGURE 6.16 | Wearable technology (wearable gadgets).

Sources: (all from public domain)
https://blog.ges.com/eu/wp-content/uploads/2015/11/wearable-technology-on-sh-012.jpg (Google Glass - public)
http://mcdullee.weebly.com/uploads/5/4/7/2/54726657/153355_orig.jpg (the wrist-device)
http://www.adweek.com/files/imagecache/node-blog/2016_Jan/ouraring-wearable-tech-hed-2016.png (the digital ring)

category includes technology devices that can be worn by a user (see Figure 6.16). These digital devices often include tracking information related to health and fitness. There are also other wearable technology gadgets in which small motion sensors are built to take photos and to make them sync with the mobile devices that we use. Another definition for 'wearable technology' or wearable gadgets is – electronics/electronic devices that can be worn on the body, either as an accessory or as part of material used in clothing. One of the main features of wearable technology is that it can connect to the Internet, enabling data to be exchanged between a network and the device.

There are three components that make the wearables 'smart' – (1) sensors, (2) microprocessors and (3) transmitters. Sensor technology is used to capture impulses from human body (of the user wearing the gadgets) or from the surroundings and sensors transform them into actionable data i.e. the convert those impulses in data on which one can act for the intended purpose. Microprocessors are used to extract, transform and load the data in a transmittable form. In this regard the RFID technology has a role to play. Transmitters are used to wirelessly send the data to cloud storage for further processing and reporting.

Refer to Chapter 7 Security in Cloud Computing where cloud security is explained.

Refer to Chapter 28 where RFID and privacy is explained.

BOX 6.9

The Amazing World of Wearware!

Like software, we now have the 'wearware'! The concept of wearable technology is related to both ubiquitous computing. Wearable gadgets, in general, have some form of (digital) communications capability; they allow the person wearing them an access to information in real time. Another feature of wearable devices (or 'wearables' for short) is data-input capabilities, that is, a provision of local data storage. There are a number of examples of wearable devices (refer to Figure 6.16) – glasses and contact lenses smart watches, smart fabrics and e-textiles, jewelry such as rings, bracelets headbands, beanies and caps and hearing aid-like devices that are designed to look like earrings.

Generally speaking, by wearable gadgets and devices, we mean the items which can be put on and taken off with ease. However, we also have now some more invasive versions of 'wearable technology' concepts – for example, the medically implantable devices or the IMDs (refer to Section 8.4 of Chapter 8). This is the case with implanted devices such as 'smart tattoos' and micro-chips. As far as the purpose of a wearable device is concerned (whether the device is worn on the body or whether it incorporated into the body) – it is to create constant, convenient, seamless, portable, and mostly hands-free access to electronics and computers.

In the fields of health and medicine and healthcare, the implications and uses of wearable technology are far reaching. These devices (i.e. the 'wearables') can create an impact in a number of areas, such as, body movements, fitness, aging, disabilities, education, music and gaming. Wearable technologies, in these fields, are used with the goal of smoothly incorporating functional, portable electronics and computers into individuals' daily lives. Earlier wearable devices were mainly used in the field of military technology. Now they are creating implications for fitness/sports and healthcare and medicine. Just about a decade back, medical engineers were thinking about wearable devices to unobtrusively monitor the health and well being of patients in the form of a 'Wearable Motherboard™' or the 'Smart Shirt,' aimed at monitoring vital signs and sending that biofeedback information to a hub station in real time – in a typical military setting. Now the scope of wearable technology is beyond our imagination!

There are five categories of wearable devices ('wearables' for short; depicted in Figures 6.16 and 6.17):

1. *Smart glasses and headgear* – one example of this is 'Google glasses' (see Figure 6.16).
2. *Smart watches* – for example, Apple and Android watches (see Figure 6.16).
3. *Fitness trackers* – for example, Fitbit, Nike FuelBand, and Microsoft Band.
4. *Wearable medical devices* – for example, system for continuous monitoring of Glucose levels in the body and the ZIO Wireless Patch.
5. *Smart clothing and accessories* – for example, smart clothing products with sensors and the OMSignal Bra.

FIGURE 6.17 | Types of wearable devices.

Sources: (all from public domain; images from top left clock-wise)
http://www.bhphotovideo.com/images/images2500x2500/apple_mj3v2ll_a_watch_smartwatch_42mm_stainless_1146124.jpg
https://2nznub4x5d61ra4q12fyu67t-wpengine.netdna-ssl.com/wp-content/uploads/2014/01/Holter-monitor.jpg
http://www.phonesreview.co.uk/wp-content/phoneimages/Flexible-Android-smartphone-transforms-into-smart-watch.jpg
https://9to5mac.files.wordpress.com/2013/09/screen-shot-2013-09-27-at-12-03-42-pm.png
http://www.talk2myshirt.com/blog/wp-content/uploads/2015/07/ecg-smart-shirt.jpg
https://assets.fitbit.com/production/surge-2016.0fd2880053305928cdaf399527734bcf.png

However, convenient as it may all sound, the wearables also bring with them security threats and privacy concerns. Wearables, which are now also in the medical domain – as the 'implantable medical devices' (refer to Chapter 8 – Smart Phone Security), continuously collect, transmit and store data. These devices handle information that is sensitive, personal, private or confidential. Given the integrated businesses operating globally, this information can be publicly available or posted in social media, where it is shared with a number of entities including unknown or un-trusted parties. By their very nature and due the very purpose for which they are used, wearable devices log vast amounts of data about the user wearing them – for example in one of the familiar device mentioned earlier, devices such as the 'fitbit' (which is a 'smart watch'; see Figure 6.17) track the data regarding the running steps of the user wearing it, the number of calories burned, heart rate and even sleep patterns. All this is only part of other information it can record about the persons using this wearable device. Wearable devices also have the capability to link the gathered information to a user profile connected to a laptop or smartphone through a Bluetooth connection and send the information to the cloud/cloud-based storage repositories. Under such a scenario, potential for a hack exists during the data exchanges. A variety of privacy concerns arise due to continuous use of wearables, because it is relatively new phenomenon. Using these devices is relatively recent and therefore, users are not aware of the potential privacy implications of continuous data collection, storage and online sharing. To illustrate the point, when someone is at your doorstep asking about your sensitive personal information and filling it in a form in front of you, at least you are aware about the type of data the person is collecting about you; but with the wearable devices you do not even know the personal data about you going to a private or a public cloud – once you click on the ubiquitous 'I agree' button, things may have already moved out of your control as far as your *personal data privacy* is concerned! The security concerns that are potentially possible with wearable devices are presented in Table 6.1. Note that the currently absent rigorous compliance requirement and regulatory requirements are also the reasons behind the insecurity of wearable devices.

TABLE 6.1 | Security threats to wearable devices

Factor for insecurity of 'wearable devices'	Remarks
Current policies for mobile device management (MDM) do not address wearables	It is not good to assume that mobile device management (MDM) policies in the organizations to deal with the 'Bring Your Own Device' (BYOD trend) are also capable of addressing security controls required for the wearables emerging in the market place. On mobile platforms it is easier to share data between apps and devices. Given that wearable gadgets function differently from smartphones, there are many unforeseen circumstances where they could pose new security risks. Simply banning or restricting certain features of wearable devices is not a sound long-term strategy. Therefore, organizations need to rethink policies, draft new plans and employ new services to deal with mobile device management.
Wireless connectivity issues	Wearable devices connect to tablets or smartphones wirelessly using protocols such as NFC (near field connectivity), Bluetooth, and Wi-Fi – this creates another potential point of entry. Some users have the tendency to leave their smartphones and Bluetooth turned on all the time now so they can sync with the wearable, but then they do not know what else could be connecting? Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack. The basic precaution for securing networks is simply to get visibility on how many connected devices there are in the vicinity.
The relative ease of physical access to (personal) data	The data stored on the local device, that is, the wearables, is often without encryption and that is a real issue. There is often no PIN or password protection, no biometric security and no user authentication required to access data on a wearable. Imagine what could happen if the device were to fall into the wrong hands (e.g., a cybercriminal) – there is a risk that sensitive data could be accessed easily.
Photos, videos and audio can be captured	Many modern wearable devices have discreet abilities in terms of video and audio surveillance surpass high-end spy gear – these were not available in the past years. It is not difficult for someone to secretly take photographs or record video or audio files using something like a smartwatch or smart glasses (see Figures 6.16 and 6.17). Clandestine capture of videos and images of sensitive areas, confidential information, is a very real possibility with wearable devices.
Non-existent or relatively weaker regulation or compliance	The manufacturers ought to address many of the security issues with wearable devices. An important issue is whether the manufacturers of wearable gadgets are to be self-regulated or to be mandated under government. In either case, organizations suffering a data breach that breaks compliance or regulatory requirements for their specific industry would find it difficult to shift the blame onto wearables; they will still be held fully accountable. Ignoring wearable device security and manufacturer or third-party app policy does not work as a defense.
Vulnerabilities and Patching	Most wearables have their own operating system and proprietary applications. The growth of wearable devices market would attract the attention of hackers and other cyber criminals. Therefore, the same precautions (of keeping the software on your desktops, laptops, smartphones and tablets fully patched and up to date to avoid the latest vulnerabilities) also apply to wearables. However, as of now neither adequate awareness about this nor insight and policy to cater for this issue seem to exist.

To conclude this section, we note that although a challenge exists with the security of wearable devices, it is not impossible to address. The rise in the use of wearables could be a real boon for devising security controls for them; organizations need to treat it more seriously rather than dismissing them simply as 'personal devices of occasional use.'

Refer to Chapter 11: Biometrics for Security.

Summary

Mobile workers take laptop computers and handheld devices outside of their organizations' secure environment. Cell phones, PDAs, smart phones, laptop computers and other devices make it convenient to access information anywhere. However, the potential for confidential information to be exploited on these devices and the ability to access corporate networks from outside the firewall, as well as the susceptibility of these devices to loss and theft, create security risks that must be addressed in order to protect your privileged data. In this chapter, we discussed the nature of mobile handheld devices and how they have the potential to create exposure to information systems security in the organizations. We emphasized and reiterated the key point that the widespread use of mobile devices as well as information explosion calls for a higher level security in the mobile devices. We also discussed security challenges in mobile and wireless computing scenario. IT departments and security professionals need to handle this issue with due seriousness warranted given the challenges faced.

Mobile devices such as PDAs and smart phones have become a key tool for traveling employees to help enable their digital lives both in the office and on the road. As more employees, including executives, begin to carry such devices, the amount of sensitive and confidential information at risk increases. While PDAs and smart phones can greatly enhance employee productivity, they can also be easily lost or stolen. Without protection, sensitive data stored on mobile devices may be breached, potentially resulting in damages, including lost revenue, regulatory penalties and loss of brand reputation and goodwill of the business enterprise. Toward the end, we provided a brief discussion on use of RFID in m-commerce. We presented the security threats and privacy concerns that come with the use of wearable technology/wearable gadgets that have the potential to connect through various options including the IoT technologies (Internet of Things).

The key point is that as mobile technology becomes ubiquitous (and wearable technology is part of ubiquitous computing), mobile security becomes increasingly important. Within the decade, mobile devices (PDAs, cell phones, wristwatches, etc.) will function as wallets, electronic banks (e-banks), business cards, proximity keys, as well as the personal information managers (PIMs) and communicators they are today.

Another key point in this chapter is that protecting the data in digital devices (including 'wearable devices' is just as important as protecting the information that flows between the device and the servers it interacts with. Device security is often something that is left up to the end user to implement and maintain. Although this is often driven by corporate policy, enterprises often look for ways to take this responsibility out of the hands of end users and place it under the enforceable control of an administrator.

Review Questions

1. Describe the changes in computing that have taken place today as compared to the past.
2. What are the 'mobility types'? Quote day-to-day examples of your familiarity that relates to them.
3. Discuss how 'perception' makes people least suspect security threats through mobile computing handheld devices. What do you recommend as some measures against this situation?
4. Explain the various measures for protection of laptops through physical measures and logical access control measures. Prepare a laptop security checklist using the guidelines provided in this chapter. Apply it to the laptop owner in your educational institute. If you are employed, then find out your organization's laptop protection policy and related procedures.
5. What is RFID? Is it an all new technology? Explain what has led to increasing use of RFID technology for protection of valuable information assets that need physical protection.

Mini Assignments

6. Take a look at the handheld device situation among the students in your institute or among the employees in your organization. Make a list of common handheld computing devices that you see being brought to your college institute/organization. Visit the websites that provide you information on the features of those listed devices. Make a study of what these devices are being typically used for. Based on this study, make a conclusion as to whether the uses of mobile handheld device in your educational institute/organization are making a full use of the features available on those devices.
7. As a way to get insights into the micro-level technical issues with mobile device security, do research on those aspects discussed in this chapter.
8. Using the Internet resources, do research on 'security architectures for mobile device designs' and produce a paper on comparative analysis of the various security design architectures.
9. As seen in this chapter, security threats are brought to the information held on mobile devices. These threats come through modern-day craze such as the media players and mobile video devices (e.g., iPods). Have a group discussion to brainstorm about what precautions organizations should take to mitigate these threats. If possible, contact organizations in your near vicinity and meet their IT departments/IT personnel to understand the policies implemented to mitigate such risks from the threat to information systems security.

Security in Cloud Computing

7

Learning Objectives

After completing this chapter you will be able to:

- understand the concept of 'cloud computing' in the context of IT infrastructure.
- appreciate the importance of cloud computing in modern IT era and know the components of IT infrastructure.
- learn about characteristics of cloud computing and deployment models for cloud.
- appreciate the benefits of cloud computing to clients.
- learn about the key aspects of security in cloud computing paradigm.
- understand the difference between 'grid computing' and 'cloud computing'.
- capture the concept of 'Big Data' in the context of cloud computing.
- learn about the Security and Privacy challenges in cloud computing.
- grasp what is meant by 'middleware'.
- understand the underlying security issues in each of the major cloud models: SaaS, PaaS and IaaS.
- take a glimpse of cybercriminal threats in cloud computing paradigm.
- understand the protection measure in cloud computing.

7.1 Introduction

In this chapter, our objective is to understand some of the *security and privacy issues associated with cloud computing*. Towards that objective, in the initial part of this chapter, the concept of *cloud computing* is explained. While the purpose of this part is to help readers who may not have had a prior idea of what cloud computing involves, the chapter is not be treated as a treatise on the topic of cloud computing. It is recommended that complete texts on cloud computing, that provide an in-depth treatment of cloud computing, should be referred. After providing the quintessential of cloud computing, the chapter embarks upon explaining the security and privacy related risks in cloud computing paradigm. We start with the *definition of cloud computing* and then we move on to explain how it works. In the last sections of this chapter you will learn about the *security and privacy problems*. This way, the chapter also serves to provide you a quick and handy summary about cloud computing, which is an important topic in itself. Keep in mind that it being a large topic, you may need to do additional reading about cloud computing depending on your level of interest in the topic.

These days cloud computing is receiving a lot of attention, both in works published (398) as well among users and yet, defining cloud computing is not easy. As per NIST (National Institute of Standards & Technology) definition: *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., services servers and networks, storage and applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction*. Thus, cloud computing is a subscription-based service wherein we can obtain computer resources

and networked storage space. Let us consider our experience with the email systems that we use. Our email client (whichever it may be – Yahoo, Hotmail, Gmail and so on) takes care of keeping and managing all of the hardware and software necessary to support our personal email accounts. When we want to access our emails, we open the web browser, go to the email client and log in. The most important piece in this is having Internet access; yet we can do it because of the 'cloud' as email system is not housed on our physical computer, we access it through an internet connection and we can access it from anywhere. Even if we are on a vacation, or at work or down the street getting coffee (at the end of tiring but satisfying shopping free!), we can check our emails – all that matters is that we have access to the Internet. Note that our email is different than software installed on our computer – such as a word processing program. When we use 'word processing software' to create a document, that document resides on the device we used to prepare it as long as we do not physically move it. An 'email client' is similar to how cloud computing works but with one difference; instead of accessing just our email, we can decide the information that we have access to within the cloud.

BOX 7.1

The Cloud: The 'What' and 'Why'?

Putting it simply, a 'cloud' is a place where information technology (IT) resources such as computer hardware, operating systems, networks, storage, databases and even entire software applications are available instantly and 'on-demand', that is, at the time when we need them. This is supposed to be almost like how we use resources like water, that is, the moment we need the water, we just need to turn the tap on (assuming, of course, that the water supply system and infrastructure is in place and works smoothly). At the same time, there also exist more complicated concepts and terms to server towards creating a definition of cloud computing; however, we need not do so. The key question is 'why do we need the cloud?' and the answer to that is simple really. We need cloud computing because with the 'cloud' (see Figure 7.1) we can do more computing tasks, we can do them faster. As the world appears to be in a constant hurry, 'speed' is the need of the hour! The next question is what do we mean by 'fast' and 'faster' compared to what? Seen from the perspective of business/organizations, they look for greater levels of productivity in work; they are bothered about reducing startup cost; they want to operate with less human resources, with less time, with less headaches and so on. Given the delays associated with traditional IT/computing infrastructure, cloud computing is supposed to overcome the problem of delayed access to IT resources like hardware, servers, development platforms and applications.

The new aspect in cloud is that it provides us a model for the use of a collection of services, applications, information and infrastructure comprising pools of compute, network, information and storage resources. These components can be rapidly coordinated, provisioned to users, implemented as per demand of the computing load, decommissioned when no more required, and can be scaled up or down. What 'cloud computing' provides us is quite simply a 'utility-like model' based on 'on-demand' allocations and consumption of IT resources. However the network still consists of the computers connected through the Internet.

7.2 Cloud Computing: Why?

NIST definition for cloud computing was mentioned in Section 7.1. In simple words, cloud computing is nothing but the delivery of computing services using the Internet. The appeal of 'cloud services' lies in that it allows individuals and businesses to use software and hardware without 'owning' the IT infrastructure because cloud services are managed by third parties at remote locations. Users of cloud services pay only for the usage based on 'how much' use they actually make of cloud services. IT Infrastructure has the following main components:

1. Computer hardware platforms
2. Operating system platforms
3. Enterprise software applications
4. Data management and storage
5. Networking/telecommunications platforms

6. Internet platforms
7. Consulting system integration services

An IT infrastructure is a complex combination of set of physical devices and software required to operate enterprise, set of organization-wide services which include computing platforms providing computing services, telecommunications services, data management services, application software services, physical facilities management services and IT management, standards, education, research and development services.

Social networking sites, online business applications (such as shopping portals which we use so rampantly), online file storage (e.g., Google drive), webmail, etc. are examples of cloud services; almost all of us use these services in our day-to-day life without realizing or consciously thinking that they are all 'cloud services'. The advantage of using the information technology infrastructure based on cloud computing model is that it allows us access to information and computer resources from anywhere that a network connection is available. Cloud computing offers us a 'shared pool of resources' – it includes computer networks, computer processing power, data storage space, and specialized corporate and user applications and more. Cloud computing has some characteristics which include (1) broad network access, (2) resource pooling, (3) on-demand

BOX 7.2

Riding on the Cloud!

Cloud computing uses the Internet infrastructure. 'Cloud' is the Internet ('cloud')-based development and use of computer technology ('computing'). The term cloud is used as a 'metaphor' (i.e., a symbol for the Internet), based on the cloud drawing used to depict the Internet in computer networks. Cloud computing is a term used for *hosted services* delivered over the Internet. There are three distinct characteristics associated with cloud service that differentiate cloud service from traditional hosting:

1. The service is sold *'on demand'* – typically the usage of the service is measured and tracked by the minute or the hour.
2. The service is 'elastic' in terms of usage – a user can have as much or as little of a service as he/she wants at any given time.
3. The service is fully managed by the provider – all that the user needs is a computing device (a desktop, a laptop, a table or a smart phone or similar devices and an Internet connection).

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet has resulted in a great demand for cloud computing. Figure 7.1 depicts 'cloud computing' concept.

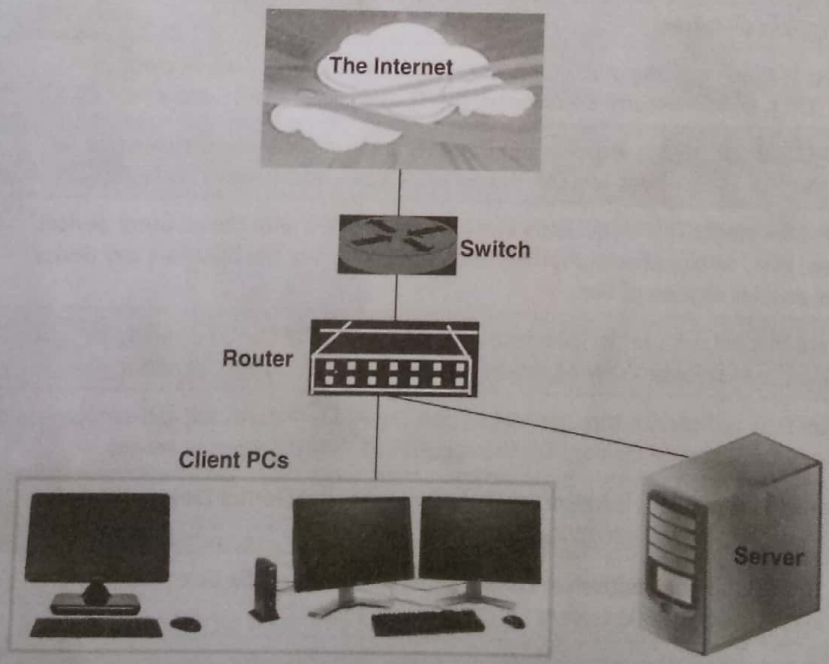


FIGURE 7.1 | Cloud computing.

self-service, (4) rapid elasticity (i.e. the service can be expanded, which means the capacity can be increased depending on the level of its use), and that it is a (5) measured service (you pay for what you used and how much use you made of cloud infrastructure). The meaning of 'on-demand self-service' is that customers (usually organizations) can request and manage their own computing resources. The use of broad network access lets cloud services to be offered over the Internet or private networks. Pooling of IT (information technology) resources allows customers to draw from a pool of computing resources, usually in remote data centers. Cloud services are 'elastic' in that they can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

Why Cloud Computing?

In the previous section, we mentioned the characteristics of cloud computing; in addition, cloud computing brings us a number of advantages (some of these have been touched upon earlier):

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

Cloud computing services can be either private or public; thus we have respectively the terminologies 'private cloud' and 'public cloud'. A *public cloud* sells services to anyone on the Internet (see Table 7.1 for cloud computing service providers).

TABLE 7.1 | Cloud computing service providers

Sr. no.	Service providers	Weblink
1.	**Amazon:** It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	**3Tera:** It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	**Force.com:** It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	**Appistry-Cloud Computing Middleware:** It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	**Microsoft Live Mesh:** This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	https://www.mesh.com/Welcome/default.aspx
6.	**AppNexus:** This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.	http://www.appnexus.com/
7.	**Flexiscale:** It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	**GoogleApp Engine:** This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	**GoGrid:** It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	**Terremark Enterprise Cloud:** It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

Source: http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-provider/ (9 October 2009).

its waste of unused processing power. Therefore, it is possible to make the physical server to 'think' it is actually multiple servers, each operating with its own independent operating system (the OS). The technique used to do this is called 'server virtualization' (see Box 7.3). Though server virtualization does not completely eliminate the need for more physical machines, it certainly reduces the same by maximizing the output of individual servers; the lesser the number of 'physical servers', the lower the IT maintenance cost.

You may like to revisit or read the chapters mentioned below:
Regarding 'protocols' (refer to Section 10.2.2, Chapter 10)
Chapter 12: Network Security in Perspective
Chapter 13: Networking and Digital Communication Fundamentals

If a company that is in the business of providing cloud services has a large number of clients, the demand for storage space is likely to be a high. Some companies require hundreds of digital storage devices. The storage requirements of cloud computing systems are large; they need at least two times the number of storage devices because they require to store data and information of their clients. That is so given that devices such as computers occasionally break down or may malfunction. A cloud computing service provider company must have a system in place to make a copy of all its clients' information and store it on suitable devices. Copies of data enable the central server to access backup machines to retrieve data that otherwise would otherwise be unreachable. 'Redundancy' is the technical term used to for making copies of data as a backup.

BOX 7.3

Virtualizing the Server

Server virtualization is considered to be one of the IT best practices. There are several definitions for 'server virtualization':

Definition 1: Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as partitions, guests, instances, containers or emulations.

Source: Definition from WhatIs.com

Definition 2: Server virtualization is the partitioning of a physical server into smaller virtual servers. In server virtualization the resources of the server itself are hidden, or masked, from users, and software is used to divide the physical server into multiple virtual environments, called virtual or private servers. One common usage of this technology is in Web servers. Virtual Web servers are a very popular way of providing low-cost web hosting services. Instead of requiring a separate computer for each server, dozens of virtual servers can co-reside on the same computer. There are several ways to create a virtual server, with the most common being; virtual machine, operating system-level virtualization, and para virtual machine.

Source: Webopedia.

In the reference section, links are provided to short video clips about server virtualization.

Cloud Computing in a Nutshell

Cloud computing is a technology whereby using the Internet and central remote servers we can maintain data and applications. Cloud computing makes it possible for consumers and businesses to use applications even if they do not have the required hardware and software installed at their end; yet they can access their personal files at any computer as long as they have the access to the Internet. In this way, cloud computing technology provides us opportunities for far more efficient computing through the use centralized data storage, processing and bandwidth.

Now let us understand about 'cloud applications' (also refer to Figure 7.5 – the conceptual view of cloud computing). There is practically no limit as to which applications can be put on the 'cloud'. To have a cloud computing system execute well all the programs on it, we just need the right middleware and with that applications of cloud computer could be run just like they would on the normal computer. Potentially, almost everything could work on a cloud computing system – from a word processing application to customized computer programs designed for a specific company. There are good reasons why would anyone want to rely on another computer system to run programs and store data. In the modern world with business running globally, clients need to access their applications and data from anywhere at any time. With cloud computing, they could access the systems/data using any computer linked to the Internet. Data now no more resides only on a hard drive on one user's computer or even a corporation's internal network. Hardware costs can be brought down with cloud computing and cloud-based computing systems are said to reduce the need for advanced hardware on the client side. Thus, one would no longer need to have the 'fastest' computer with the 'maximum' memory. This is so because the cloud system would address all of those needs. Instead, all one needs is an inexpensive computer terminal. The terminal needs to simply have a monitor, input devices like a mouse and a keyboard along with just adequate processing power to run the middleware with which to connect to the cloud system. We will not even need a large capacity hard drive because with 'cloud' we now store all our information on a 'remote' computer.

To achieve their computing goals, organizations that have dependability on computers ought to ensure they acquire the right software. Through cloud computing systems the employees and other stakeholders of the organizations get company-wide access to computer applications. What is more, for the company it is no longer obligatory to buy a set of software or software licenses for every employee. All that the company needs to do is to pay a metered fee, that is, adapt to a 'pay-as-you-go' model to pay a cloud computing company based on the actual usage. However, 'space' is still an issue because digital storage devices and servers do occupy space. Therefore, some companies may need to rent 'physical space' to store the data in their databases and servers which otherwise would not be available on site. To the organizations that have such a need, the providers of cloud computing services provide the option of storing their data on someone else's hardware, thereby eliminating the need for physical space upfront. In a scenario that there are lesser number of physical machines under a cloud computing scenario, another advantage of cloud computing is that organizations might save money on IT support. In theory at least, efficient hardware would have fewer problems than a network consisting of *heterogeneous computing* devices and a plethora of operating systems. Often, the work of scientists and researchers involves complex calculations; so complex that it would take years for computers to complete them. Using a grid computing system, the client could send to the cloud the calculation for processing. The cloud system would utilize the processing power of all available computers on the back end, greatly speeding up the calculation.

BOX 7.4

Grid Computing

For the term 'grid computing', a number of definitions are available. For reader reference a few definitions are quoted here. Grid computing is a distributed architecture of large numbers of computers connected to solve a complex problem. In the grid computing model, servers or personal computers run independent tasks and are loosely linked by the Internet or low-speed networks. Computers may connect directly or via scheduling systems. (For further reading see, http://searchdatacenter.techtarget.com/definition/grid-computing)

By 'Grid' we mean an infrastructure that enables the integrated, collaborative use of high-end computers, networks, database and scientific instruments owned and managed by multiple organizations. (Peter Lee, IBM IT Specialist)

Basically, the 'Grid' is the suite of 'computer utilities', designed to service individual homes and offices across the country just like our electric and telephone utilities do for us. Carl Kesselman, Ian Foster and Steve Tuecke were the first ones to establish the idea of grid computing way back in the early 1990s. They are the trio who developed the standard for Globus Toolkit and that included grids for data storage management, data processing and extensive computation management. Grid computing is a processor architecture that pools computer resources from many domains to reach a main objective. In grid computing, the computers on the network can process a task together, thus functioning as a supercomputer. Although, normally, a grid handles a number of tasks within a network, it can also work on specialized applications. The grid is designed to solve problems that are too complex for a supercomputer and also to handle computing scenarios wherein there is the need to have the flexibility to process many smaller problems. Thus, by their very nature, computing grids provide us a multiuser infrastructure to manage the demands of large information processing which are not regular in their needs.

BOX 7.4 (Continued)

Conceptually, a grid is network connected by parallel nodes to form a computer cluster. Such a cluster uses an operating system to run it, for example Linux or some other free software. The size of the cluster can vary ranging from a small work station to several networks. Grid computing technology today is applied to several applications, such as mathematical or scientific computing or even in e-learning settings that need to make use of several computing resources for educational purpose. Grid computing is also used in structural analysis, back-office infrastructures, ATM banking that is based on Web services and in the fields of scientific or marketing research.

It is important to understand the difference between 'grid computing' and 'cloud computing': see the vignette below.

Cloud Computing is similar to but not same as *Grid Computing*

It is important to understand the difference between 'grid computing' and 'cloud computing' – the two terms are related but the not the same. Cloud computing is comparable to grid computing, but with a small difference; whereas the whole grid acts like a 'Virtual Supercomputer', in cloud computing this virtual entity, that is, the cloud, is not built upon one, but several grids on different physical locations and resources are shared between smaller instances of computing, that is, the 'virtual instances'. Organized this way, each 'instance' of computing can be executed on different locations (in proximity to the client) and can, therefore, reap benefits of large grids which are nothing but efficient with scalable and flexible workloads.

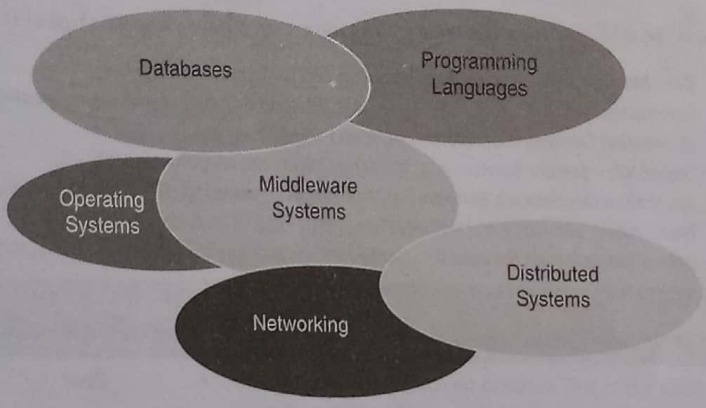


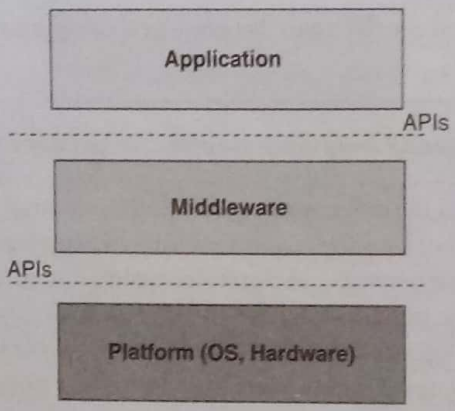
FIGURE 7.3 | What and where of 'Middleware'.

Now let us understand the role of 'middleware' in modern computing systems (refer to Figure 7.3). In simple words, middleware is about supporting the development of distributed applications in networked environments. This also includes the integration of systems. Middleware is used to make computing tasks easier, more efficient and less error-prone. It is also about enabling the infrastructure software for this task. Middleware systems are the abstractions and services to facilitate the design, development, integration and deployment of distributed applications in heterogeneous networking environments. In modern computing, software technologies are used to help manage complexity and heterogeneity inherent to the development of distributed systems, distributed applications and information systems. Middleware is the layer of software that exists above the operating system and the network substrate, but below the application layer. Middleware is the higher-level programming abstraction for developing the distributed application. It is something that conceptually operates at a layer that is higher than 'lower' level abstractions, such as sockets provided by the operating system (a socket is a communication end-point from which data can be read or onto which data can be written).

BOX 7.5

Middleware

We can look upon 'middleware' as the 'glue' that connects varied computer systems. Usually, information in proprietary formats is stored in 'legacy systems' and legacy systems use propriety protocols to communicate, and may even be running on hardware that is no longer manufactured or supported. In other words, middleware is connectivity software that has a set of enabling services that allow multiple processes to run on one or more computers that are connected with each other. In technical terms, *middleware services* are nothing but sets of distributed software that exist between the application and the operating system and network services on a system node in the network. A conceptual diagram showing the three layers (involving the middle layer) is depicted in Figure 7.4.



OS: operating system, API: application program interface

FIGURE 7.4 | Middleware.

There are several types of middleware categories; each provides a specific type of service as mentioned below:

1. *Data Management Services* (i.e. Database and file system middleware).
2. *Communication Services* [i.e. RPC (Remote Procedure Call) and messaging middleware].
3. *Distribution Services* (i.e. location, time and security services).
4. *Object Management Services* [i.e. by using Object Request Brokers (ORBs)].
5. *Application Co-operation Services* [i.e. Transaction-Processing (TP) monitors, e-mail, etc.].
6. *Presentation Services* (i.e. User Interfaces, printing and multi-media middleware).
7. *System Management Services* (i.e. Configuration-, change-, operations-, problem-, and performance-management services).

7.4 Conceptual View of Cloud Computing – Characteristics and Deployment Models

As mentioned in Section 7.2, the characteristics of cloud computing are: (1) broad network access, (2) resource pooling, (3) on-demand self-service, (4) rapid elasticity (i.e. the service can be expanded which means the capacity can be increased depending on the level of its use), and that it is a (5) measured service (you pay for what you used and how much use you made of cloud infrastructure). A conceptual view of cloud computing is presented in Figure 7.5 – as we can see in the light of the discussion so far, there is a heterogeneous IT infrastructure with a conglomerate of hardware.

Deployments for the Cloud

There are 11 major types of categories or 'models' or 'patterns' to implement cloud computing technology. In Table 7.2, we provide a brief description of each. It is more common to talk about only IaaS, SaaS, PaaS, etc.; however, we provide a much wider overview to our readers so that they appreciate the extensiveness of cloud services.

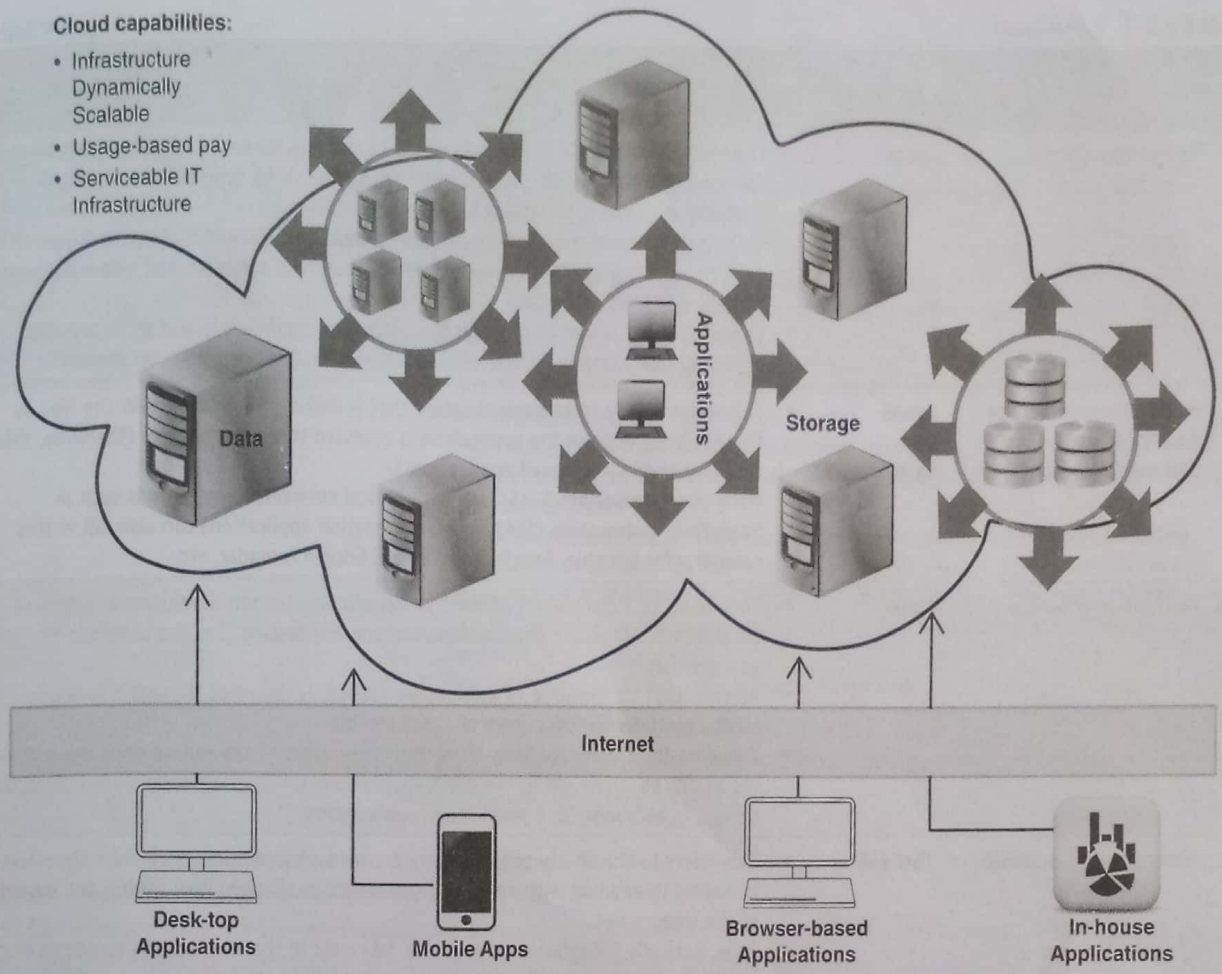


FIGURE 7.5 | Conceptual view of cloud computing.

TABLE 7.2 | Categories of cloud computing technology

Name of the category (Cloud computing)	Short name	Brief description
1. *Storage-as-a-Service*	SaaS	• This works as 'disk space on demand'. This is the ability to use the physically available storage that is available at a remote site but is treated logically as a local storage resource to be used by any application that requires it, that is, the storage. • This is the most primitive component of cloud computing. • This component is most used by other cloud computing components.
2. *Database-as-a-Service*	DaaS	• This provides the ability to use the services of a database that is remotely hosted so that it can be shared with other users. • At the same time, it functions as if logically it were a *local database*. • Different service providers have different models to provide the DaaS service; nonetheless, the central idea is to reap the power to use database technology that would otherwise cost a very high amount of money in duplicating hardware and procurement of software licenses.
3. *Information-as-a-Service*	InfOaaS	• By this, we mean the ability to consume any type of remotely hosted information through a well-defined interface such as an API (application interface). • Examples: Customer address validation, stock price information, credit reporting, etc.

TABLE 7.2 | (Continued)

Name of the category (Cloud computing)	Short name	Brief description
4. *Process-as-a-Service*	**PRaaS**	• This refers to a remote resource that can bind many resources together, such as service and data, whether hosted within the same cloud computing resource, or remotely available – to establish business processes. • We can think about a *business process* as a 'meta application' that spans across systems, leveraging key services and information that are combined into a sequence to form a process. • Changing these *processes* is easier than changing *applications* and so, it provides agility to those who use these process engines that are delivered 'on-demand'.
5. *Application-as-a-Service* Also known as *Software-as-a-Service*	**APaaS OR SaaS**	• This refers to any software application that is delivered to a user, over the Web as the platform, wherein the application is accessed through a browser (therefore, this category covers web-based applications). • Many people associate AaaS/SaaS with typical enterprise applications such as Sales Force Automation (SFA). Office Automation applications can also fall in this category; for example, Google Docs, Gmail, Google Calendar, etc.
6. *Platform-as-a-Service*	**PaaS**	• This works as a complete 'platform'. It includes application development, interface development, database development, storage and testing (i.e. the complete lifecycle as a service). • All this, that is, the suite of services mentioned, is delivered through a remotely hosted platform to subscribers of cloud service. • Based on the traditional 'time sharing' model, modern PaaS service providers provide the ability to create enterprise-class applications for local use or as an 'on-demand' service in exchange for a small fee or subscription.
7. *Integration-as-a-Service*	**IntGaaS**	• This refers to the ability to completely deliver an 'integration stack' from *the cloud*, including interfacing with application, semantic mediation, flow control and design of the integration. • Thus, basically 'integration as a service' has most of the features and functions that we find in traditional EAI technology; however, they are delivered as a service. **Note:** The security aspects of EAI are presented in Chapter 37 – it is available on the CD companion of the book.
8. *Security-as-a-Service*	**SeCaaS**	• This is the ability of the cloud technology to deliver 'core security services' remotely, using the Internet. • Although currently, only rudimentary security services are provided, over a period of time, more sophisticated security services are being made available, such as 'identity management'. **Note:** In the reference section a few links are provided where you can read more about *security services delivered through the cloud*.
9. *Management/Governance-as-a-Service*	**MgGoVaaS**	• This is any 'on-demand-service' that provides the ability to manage one or more cloud services. • Typically, there are simple things such as 'topology' (see Chapter 13; Network Topologies are explained in Section 13.4), resource utilization, virtualization and uptime management (from service delivery perspective, 'uptime' is important; you may like to refer to Chapter 22 where the ITIL model is explained in brief). • IT Governance systems are also now becoming available as well through the cloud – such as the ability to define and enforce IT security and data privacy related policies. **Note:** 'Data privacy' is becoming the basic IT hygiene in view of globalization business. Defining a (data) privacy policy is the fundamental best practice; you may like to visit Section 28.7 of Chapter 28 where some best practices are discussed from data privacy perspective.

TABLE 7.2 | (*Continued*)

Name of the category (Cloud computing)	Short name	Brief description
10. Testing-as-a-Service	TaaS	• This is the ability to test local or cloud delivered software systems/applications testing software and services that are delivered remotely using a server that is remotely hosted. • Note that while the 'cloud service' itself needs to be tested, 'testing-as-a-service' systems can test other cloud applications, websites, and internal 'enterprise systems'. This they can do without requiring a hardware or software footprint within the enterprise.
11. *Infrastructure-as-a-Service*	IaaS	• This refers to setting up Data Centers as a service; in other words, the capability to remotely access computing resources. • Under this type of cloud service arrangement, basically, you lease a 'physical server' that you can use as you wish. For all practical purposes, it is 'your' data center or at least part of a data center. • The difference between this approach and the more mainstream cloud computing is that instead of using an interface and a 'metered service' (to measure the extent of your usage of the cloud service), you are getting access to the entire machine and the software on that machine (typical to call that machine a 'box'; meaning the hardware in that data center). • Thus, it is less 'packaged' and more akin to hosting.

What Cloud Computing IS and IS NOT

Although cloud computing is an emerging field, the idea has been evolved over few years. It is called cloud computing because the data and applications exist on a 'cloud' of Web servers.

Cloud computing is when *application* and *data* are not confined to any specific company's server or no VPN access and when it encompasses multiple companies, multiple servers and multiple networks.

Cloud computing IS:

A style of computing where massively scalable IT-enabled capabilities are provided 'as a service' over the network. Cloud computing encompasses multiple companies, multiple servers and multiple networks.

Cloud computing IS NOT:

Network Computing; nor it is traditional outsourcing. It is *not* a contract to host data by third-party hosting business; nor is it subcontracting for computing services for specific outside firm.

With cloud computing, *application* and *data* are not confined to any specific company's server and there is no VPN Access.

Cloud Deployment Models: *Public, Private, Community* and *Hybrid*

It is important to understand these key terms. A *public cloud* has two basic characteristics:

1. Public availability of the cloud service offering.
2. The use of public network to communicate with the cloud service.

Very large resource pools are used to procure cloud services and cloud resources. These resource pools are shared by all end users. These resource pools are like 'IT factories' (IT is information technology), which tend to be especially built for running cloud computing systems to provision the resources precisely according to required quantities. The provider of cloud services can achieve significant economies of scale by optimizing IT operation, IT support and IT maintenance. Therefore, it leads to low prices for cloud resources, which in turn, works to the benefit of cloud service users. Additionally, public cloud portfolios employ techniques for resource optimization. Interestingly, these aspects are transparent as far as the end users are concerned. However, this mode of working may represent a potential threat to the security of the system. If a cloud provider runs a number of data centers, IT resources can be assigned in such a way that the load is uniformly distributed between all centers. Figure 7.6 depicts the concept of 'public cloud'; it shows users accessing a public cloud.

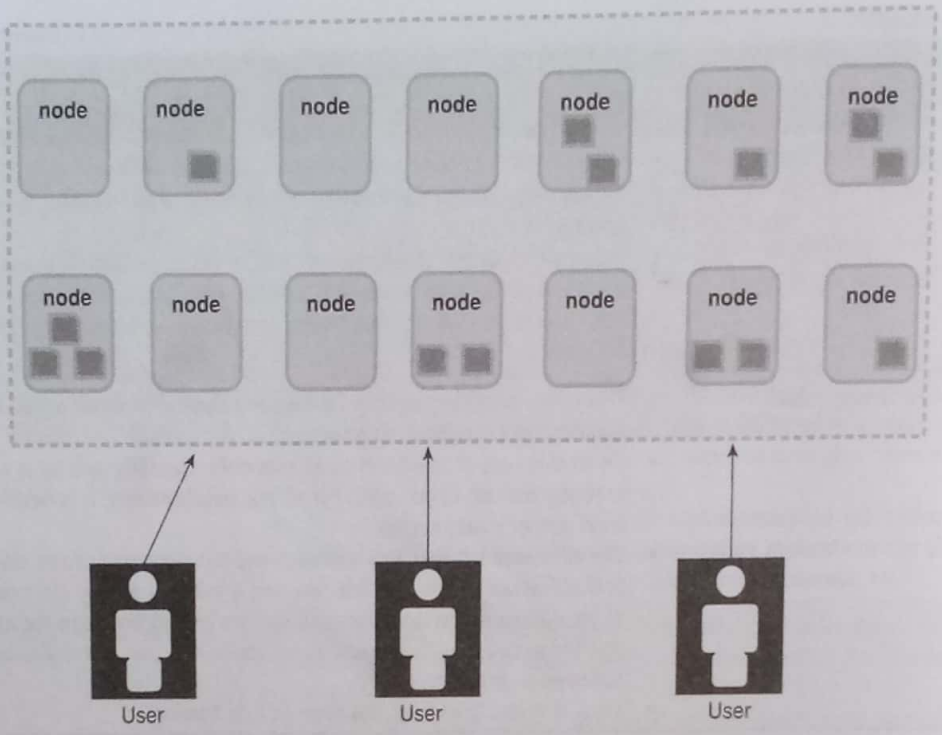


FIGURE 7.6 | Public cloud access.

Node

A node is a system or device connected to a network. As an example, if a computer network connects a file server, seven computers and three printers, the network is said to be consisting of 10 nodes. Each device on the network has a network address, such as a MAC address (Media Access Control Address) to uniquely identify each device. Using the MAC address, we can keep track of the data destination, that is, where data is being transferred to and data source, that is, from which network the data comes. Note that, sometimes, node can also refer to a leaf, which is a folder or file on a hard disk.

Now let us understand the concept of *private cloud*. Private cloud computing systems mimic a public cloud service offering except that it operates within the boundaries of an organization. business applications and offered services are accessible only for one designated organization. Virtualization solutions are used by private cloud computing systems and the focus is on consolidating distributed IT services typically within data centers owned by the company. The main advantage of private cloud systems is that the given company (i.e., business organization) keeps full control over corporate data, security guidelines and system performance; this way information security and data privacy risks are minimum. As a down side, private cloud offerings are not comparable in scale, that is, private clouds usually are not as large scale as public cloud offerings. This results in not being able to reap the benefits of economies of scale. Figure 7.7 depicts the concept of 'private cloud'; it shows a user accessing a private cloud.

Now let us understand the concept of 'community cloud'. A community cloud scenario involves organizations that have the need to share a cloud infrastructure. Community cloud can be understood as a 'general private cloud', that is, a generalization of a private cloud concept where (as explained) a private cloud is an infrastructure that is accessed by only one particular organization.

Yet another deployment model is that of a hybrid cloud. In a hybrid cloud, service deployment mode implements the required processes by combining the cloud services of different cloud computing systems, for example, private and public cloud services. The hybrid model is also suitable for enterprises in which there is a scenario of transition to full outsourcing that has already been completed An example of this is combining community cloud services with public cloud services or combining all the three types: private cloud, public cloud and community cloud. Figure 7.8 depicts the concept of 'hybrid cloud'; it shows users accessing a combination of the three clouds.

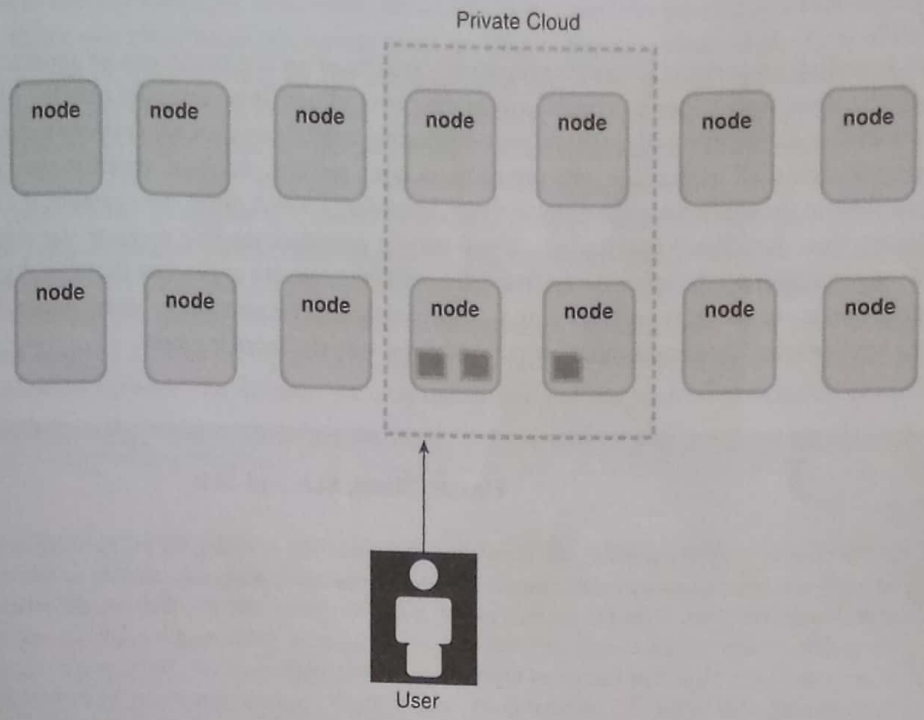


FIGURE 7.7 | Private cloud access.

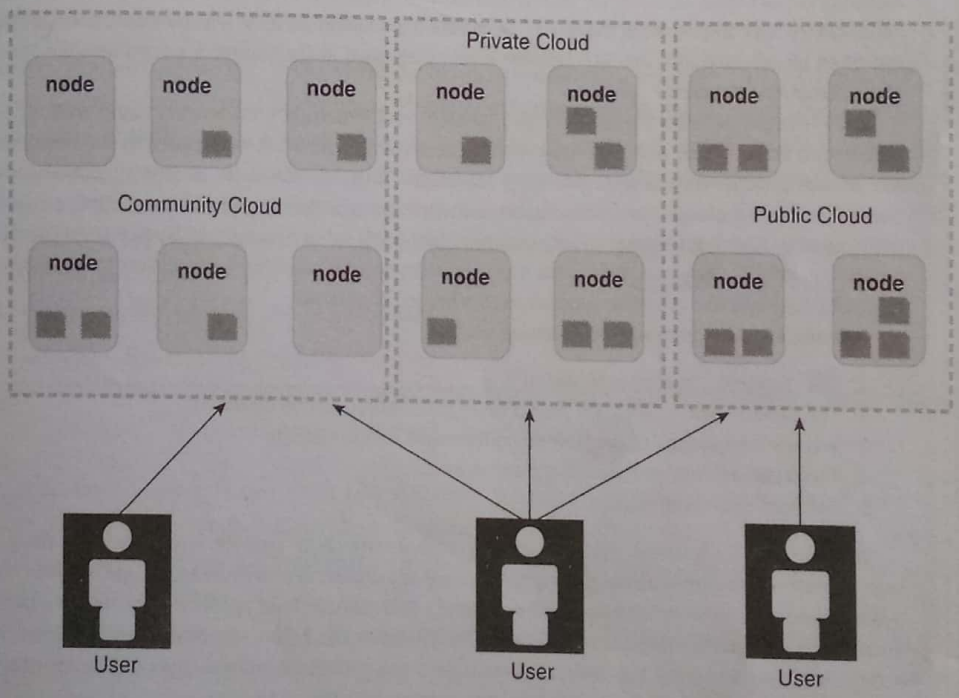


FIGURE 7.8 | Hybrid cloud access.

Cloud: Elasticity and Availability

The two important characteristics of cloud computing are (1) elasticity and (2) availability. Let us now briefly consider the two characteristics of the cloud; namely *elasticity* and *availability* (recall the discussion in Chapter 4 – 'availability' is one of the three pillars of information security; see Figure 4.3 in Section 4.4 of Chapter 4). Let us discuss *cloud elasticity*.

Cloud Elasticity

Elasticity is the most appealing proposition of cloud computing – it is based on the 'pay as you go' model. Under this model, the payment made by the cloud service user is proportional to the extent of use. Thus, one pays only for what one uses. What this implies is that depending on the type and extent of your computing requirement, an application in cloud can grow bigger and contract 'on demand', across all its tiers (i.e., the presentation layer, services, database, security; see Table 7.2). This also means that the components of the application can grow without depending on each other. For example, if a business enterprise needs additional storage space (in cloud) for database, cloud service providers are able to grow the database tier without impacting, changing or reconfiguring the other tiers. Under this paradigm, we can appreciate that cloud applications are like a sponge; the sponge grows in size when we add water to it, and contracts as we remove the water. Extending the analogy to the world of business applications, this means the more customers we add, the more it grows.

BOX 7.6

Elastic Cloud, SLA and SLO

In the domain of cloud computing, the term 'elasticity' is used for indicating the extent or, let us say, the degree to which a software system (or a particular cloud layer) autonomously adapts its capacity to adjust to the workloads that change over time. Given the dynamic nature of today's businesses, this is a very desirable attribute of cloud computing models. In the context of cloud computing, 'capacity' refers to the maximum workload a system (or a particular cloud layer) can handle as bound by its service level objectives. By 'elastic computing' we mean the dynamic adaptation of capacity; in other words, altering the use of computing resources to meet a varying workload. According to the IT giant organization IBM, 'elasticity is basically a "rename" of scalability [. . .]' and 'removes any manual labor needed to increase or reduce capacity'.

In the cloud computing context, *elasticity* is a critical characteristic that differentiates cloud computing from other computing paradigms, such as grid computing (refer to Box 7.4). An "elastic" cloud application or process has three elasticity dimensions: (1) cost, (2) quality and (3) resources and all the three need to be enabled to increase and decrease its cost and enhance the quality, or available resources, so as to accommodate specific requirements which are often closely tied with the SLA (service level agreement) in the contracts signed with the vendors who provide cloud computing services.

In the context of 'elasticity' of the cloud, another very important term to understand is 'SLA'. SLA (service level agreement) is important when, for transitioning, application support is outsourced by the customer organization to the service provider organization through a 'contract'. Thus, an SLA is an electronic contract/contract between a service user and a provider, and specifies the service to be provided, Quality of Service (QoS) properties that must be maintained by a provider during 'service provision' [generally defined as a set of Service Level Objectives (SLOs)], and a set of penalty clauses specifying what happens when service providers fail to deliver the QoS agreed. Not meeting the SLAs may lead to a situation amounting to a breach of contract.

Typically, an SLA addresses the following points:

1. The availability of service to users.
2. The performance targets (for the software system/application delivered).
3. The operating range of guaranteed performance and availability.
4. The measurement and reporting mechanisms.
5. The cost of service provided.

With the term SLA comes the other closely related term 'SLO' (service level objective). While an SLA (service-level agreement) is a contractual binding to outline a specific service commitment made between contracting parties (typically two – a customer and its service provider), SLO (service level agreement) comes into picture when we talk about the performance metrics (for measuring the effectiveness of the service delivery). Thus the individual metrics established for measuring the delivery performance are called the service level objectives (the SLOs). Thus we generally do not have the SLOs in isolation; they come in with the SLAs.

Pure IaaS providers (refer to Table 7.2) provide certain benefits, in particular, the operating costs; however, an IaaS provider will not help towards making the users' applications 'elastic'; even 'Virtual Machines' will not help. A server (physical or virtual) is the smallest elasticity unit of an IaaS provider . Adding servers in a data center (refer to 'IaaS' in Table 7.2) helps in achieving scale, although it is hardly enough. The application has yet to use this hardware. Most important, if the process of adding computing resources is not transparent to the application, the application is not elastic. In other words,

there should be the ability to expand the computing infrastructure without the user being aware of it; as if it is all done in the background with the sole objective of supporting users' growing computing need. In the light of the description so far, we see that designing the IT infrastructure for the cloud is not about 'more servers'; it is about designing an application for elasticity regardless of the underlying server farm. The term 'server farm' refers to a collection of computer servers that are usually maintained by an organization in order to achieve server functionality that extends far beyond the capability of a single machine. Often server farms are made of thousands of computers which require a large amount of power to run and huge air conditioning arrangement to keep them cool. Even to achieve an optimum performance level, a server farm has enormous costs associated with it, both financially and environmentally. Server farms also need 'backup servers' (based on the disaster recovery principle – explained in Chapter 31). Backup servers are meant to take over the function of primary servers in the event of a primary-server failure. Server farms are typically collocated with the network switches and/or routers (refer to Chapter 13: Networking and Digital Communication Fundamentals). Switches and routers are needed to enable communication between the different parts of the cluster and the users of the cluster. Server farms are typically found in data centers.

Next, we discuss the second most important attribute of a cloud service, namely, availability.

Amazon Web Services: An Example of 'Elastic Cloud'

1. Computing resources are rented by the hour.
2. Basic unit of computing = instance hours.
3. Additional costs for extra bandwidth are paid.
4. Uses persistent storage.
5. Service is charged by the Gigabytes per month.

Cloud Availability

As mentioned before, 'availability' is one of the three pillars of information security. This attribute (i.e., availability) comes from the business emergency that is thrust upon us by global businesses and the rise of electronic commerce and digital assets (the concept of 'IT assets' is explained in Chapter 34). As explained in Section 4.4 of Chapter 4, the concept of 'availability' ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, 'availability' guarantees that the systems are up and running when they are needed – refer to Figure 4.3 (the C.I.A. triad) of Chapter 4. In reality, however, as much as we may like it that way, making applications highly 'available' is very difficult. It requires highly specialized tools and trained staff. On top of it, it is also quite expensive to provide the commitment of 24 × 7 available applications (refer to the concept of SLA and SLO explained in Box 7.6).

Types of Cloud Services

1. **Infrastructure-as-a-Service (IaaS):** It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an API from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
2. **Platform-as-a-Service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. Google Apps is one of the most well-known PaaS service providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.
3. **Software-as-a-Service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from web-based E-mail to applications such as Twitter or Last.fm.

Table 7.2 has a far larger list of types of cloud services, while the cloud services mentioned here are the most common ones.

BOX 7.7

Hot, Warm Cold Sites for Disaster Recovery and Other Similar Arrangements

Cold sites: These are offsite pre-configured facilities that have the necessary utilities and TC power to support a computer system. Cold sites have only the basic environment (electric wiring, air conditioning, flooring, etc.) to operate an information processing facility (IPF). The cold sites are ready to receive equipment but do not offer any components at the site in advance of the need. Activation of the site may take several weeks. Therefore, for cold sites, it is important to assess low-cost access versus time to obtain, install and test a new system.

Warm sites: These are partially configured, usually with network connections and selected peripheral equipment, such as disk drives, tape drives and controllers, but without the main computing equipment. Sometimes a warm site is equipped with a less powerful central processing unit (CPU) than the one generally used. The 'warm site' has an assumption behind it that the computing equipment can usually be obtained quickly for emergency installation and since the computer is the most expensive unit (i.e., mainframes and mid-range computing facilities), such an arrangement is less costly than a hot site. After the required installation has been done, the site can be ready for service within hours. However, the location and installation of the CPU and other missing units could take several days or weeks.

Hot sites: These are stationary or ambulant facilities containing all the backup support of a cold site plus a similar/identical operational computer system to the one at the primary site. Thus, hot sites are fully configured and ready to operate within several hours. The equipment and system software at the hot site must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation. Costs associated with the use of a third-party hot site are usually high but often the cost is justifiable for critical applications of the organization (recall the discussion on the 'strategic grid' proposed by McFarlan and McKenney in Section 31.2 and Figure 31.3).

It is important to appreciate that the hot site is intended for emergency operations of a limited time period and not for long extended use. Therefore, the hot site should not be viewed as a means of accomplishing the continuation of essential business operations for a period of up to several weeks following a disaster or a major emergency. Components of the DR plan for network connectivity to a hot site over a public-switched network should address such issues as redundancy and maintaining sufficient capacity on diverse paths to carry a re-routed path. They should also provide for late night access routing through different central offices so that no single point of failure can impact the entire network.

In some businesses, due to high availability requirements, it becomes mandatory or highly necessary to run multiple data centers and often they are run under the IaaS model of cloud (refer to Table 7.2). In some business enterprise, some data centers are simply on standby (refer to the concept of cold, warm, hot, and sites explained in Section 31.7 of Chapter 31), waiting to be used in case of a failover. Other organizations strive to achieve a certain level of success with active data centers, in which all available data centers serve incoming user requests. While achieving high availability for services is relatively simple, establishing a highly available database server farm is far more complex. Its high level of complexity makes organizations establish yearly tests to validate failover procedures. The importance of disaster recovery is underlined in Chapter 31.

In the context of 'cloud security', disaster recovery is of utmost importance. The importance of disaster recovery is underlined in Chapter 31.

To some extent, some IaaS providers can provide support to a business organization's complex disaster recovery planning (for the details of DRP, refer to Chapter 31) and setting up data centers (under the IaaS model of cloud computing; refer to Table 7.2). Under such an arrangement, it is possible to achieve successful failover. However, the onus of the operational aspects of the disaster recovery still remains with the business organizations to manage and maintain such an environment unless, of course, the entire IT maintenance work has also been outsourced to a third-party vendor, including regular hardware and software upgrades. Cloud computing, on the other hand, takes away the need for most of the disaster recovery requirements by hiding many of the underlying complexities.

It is important to understand the difference between 'grid computing' and 'cloud computing' – the two terms are related but are not the same. Cloud computing is comparable to grid computing, but with a small difference – see Box 7.8.

BOX 7.8

Cloud Computing, Grid Computing

The underlying concept in *Green Computing* is that of building computing centers and data centers that are environmentally sustainable and environmentally friendly. These are known as 'green data center' (although such a concept remains only euphoric as of now but awareness towards achieving them is on the rise). *'Green' Data Centers* are supposed to have lower power consumption which in turn aids in reduced CO_2 emission levels, etc. Thus, the main objective is being 'energy efficient' as much as possible with great concern for the environment. However, at times, this limits the possibility of handling any workload size due to limited resources.

Grid computing is a concept is based on establishing a number of computing centers and data centers that do not have the aim of being environmentally friendly and efficient, but instead to be modular and to have a large number of independent units which can be turned on and off to handle large and smaller workloads efficiently. Thus, the main concern in grid computing is being able to scale up and down in order to be able to handle any possible workload equally efficiently, regardless of resources and the environment – in that sense, we see that there is 'elasticity' (the term explained in Box 7.6).

Cloud computing and *grid computing*, though similar, are not exactly the same. Whereas the 'Grid' acts like a 'Virtual Super Computer', in cloud computing this virtual entity is 'the cloud' and it is built upon not a single grid, but rather several grids established at various physical locations and computing resources are shared between smaller 'virtual instances'. In this manner, each instance of computing can be carried out at different locations (placed as close as possible to the client). Each instance can share benefits of large grids (efficient with scalable and flexible workloads, that is, 'elasticity' – refer to Box 7.6).

Thus, the main objective is being flexible in terms of scalability so that instances use only those resources that are indeed required, nothing more than those needed, so that is should be possible maintaining the possibility of assigning more resources quickly if workloads begin to fluctuate in order to maintain the same level of efficiency. Similar to grid computing, clouds seldom care for environment-friendly ideologies. Their main imperative is to be dependent, efficient, flexible, scalable and 'always available'.

7.5 Big Data and Cloud Computing

Now-a-days, big data is one of the most hyped and least known areas of the cloud ecosystem. People wonder whether big data and cloud are two different areas all together and if both may work together.

Big data is all about extracting VALUE out of 'variety, velocity and volume' (the three Vs) from the information assets available whereas cloud focuses on attributes such as (1) on-demand service, (2) elastic, scalable, (3) pay-per use self-service models. So the question is: What is the relationship between cloud and big data? Why should we discuss these two entirely different areas together?

Refer to Chapter 34 about IT Asset Management; the concept of 'information asset' is explained there.

Those who have used 'Elastic Map Reduce' on Amazon would appreciate an evident aspect of this relationship. Big data need large on-demand compute power and distributed storage to address the 3 Vs (variety, velocity and volume) data problem and cloud seamlessly provides this elastic on-demand compute required for the same. 'Apache Hadoop' is the de-facto standard for big data processing, and with this standard, the big data processing has become more batch oriented in its current state. The unpredictable workload nature of the big data computing infrastructure makes it a true case for the cloud. Amazon's 'Elastic Map Reduce' shows us how big data processing can be done by taking advantage of the power of cloud's elastic computing power. Note, however, that this may not be the only part of this relationship between cloud and big data because, on a closer look, the other patterns of this relationship emerge.

HADOOP related links are provided in the reference section at the end of the chapter.

Cloud has been hyped as the 'As-a-Service' model (refer to Table 7.2) – this is mainly due to the 'transparency' offered by hiding the complexity and challenges involving in building a scalable elastic self-service application. Big data processing

has the same requirement. Hadoop (the standard mentioned earlier) works in a similar way by hiding the complexity of the large-scale distributed processing from the end user perspective. The users write 'Map-Reduce' programs or use other similar programming constructs in order to seamlessly perform the big data crunching without worrying about fault-tolerance elasticity, node failures, linear scalability, process/data replication, etc. While all this is taking place, behind the screen, Hadoop provides the large-scale distributed capabilities. Thus, the simplification provided by cloud and big data is the main reason for the extensive adoption of big data and cloud. One example of such successful adoption is Amazon – it demonstrates how this simplification, provided by the combination of cloud and big data, can increase the adoption of a seemingly complex problem of large-scale distributed processing.

Big data and cloud computing both are aimed at delivering value to enterprise by lowering the cost of ownership. Cloud makes this possible through the pay-per-user model turning capital expenses (CAPEX) into operational expenses (OPEX). As an example of this, note that the licensing cost is brought down through the use of Apache open source and a sophisticated solution – it would have otherwise cost millions to build or buy the solution. Both big data and cloud has been driving the cost down for the enterprise and thus bringing VALUE to organizations that embrace the cloud computing model. Early adopters of the big data are moving away from the 'traditional licensing models' to open-sourced model and thus lowering the overall processing cost (Cost per Terabyte or CpTB). This is how both cloud and big data deliver value to businesses by streamlining their IT operations in the process. With the marriage between cloud and big data, the days of 'Analytics as a Service' are heralded; however, both cloud computing and big data bring in data security and privacy concerns.

BOX 7.9

'Green' Cloud

In simple words, Green Cloud refers to energy-efficient cloud computing. So the question is about keeping your cloud computing green, that is, 'clean' – making use of 'clean energy'. Environmental consciousness is growing, given the climate changes that are taking place on our planet. Greenpeace is a group dedicated to environmental issues. In May 2011, this group released a report evaluating the energy choices of some of the big Cloud companies, like HP, Microsoft, Amazon Web Services, Google and IBM. The idea was to compare the energy-related footprint of major providers and their data centers. According to Greenpeace, although there has been a proliferation of industry-created metrics for sustainability, no answers could be sought to questions such as: how much dirty energy is being used, and which companies are choosing Green energy to power the Cloud? It was argued that economical use of fuel may not be equivalent to a diminished consumption – it was felt that it could be a contradiction!

For those who are interested in reading the full report, links are provided in the reference section at the end of the chapter.

7.6 Security and Privacy Risks in Cloud Computing

Two of the biggest concerns about cloud computing are information *security* and data *privacy*. Business process outsourcing being at a peak in today's global businesses, it is indeed a worrisome matter handing over important data to another company. The potential for the misuse of shared confidential data always exists. Often, people in the corporate world, that is, executives in large organizations are known to hesitate to reap the benefits of a cloud computing system because they, with data going to the cloud, fear the loss of control over it; they can no more keep their business sensitive/confidential data and information under lock and key.

Data Privacy, Business Privacy, Data Sensitivity

For a basic grounding on these topics, you may like to refer to the chapters of this book mentioned below:

Chapter 27: Privacy – Fundamental Concepts and Principles

Chapter 28: Privacy – Business Challenges and Technological Impacts

It is important to distinguish between 'information security' and 'data privacy' – in this regard, you may like to visit the chapters of the book mentioned above. There is of course, a counterargument to the risk of losing data privacy and it lies in

believing that the companies who offer cloud computing services are bothered about keeping their reputations. Therefore, it must be in the interest of these companies to have in place reliable security measures. Without such measures, the cloud computing service businesses would lose all their clients. Therefore, they often employ the most advanced techniques towards the protection of their clients' data. Thus, the security and privacy of personal information is of utmost importance when it comes to cloud computing. Given that personal information is being shared with another organization, often beyond the border of a country, it is vital to ensure that the information is safe and that it is being accessed only on the basis of CBN (continued business need); in other words, ensuring that only 'authorized persons' are able to access it. The risk lies in that the personal information sent to a cloud provider might be retained for a period longer than called for or be used for other purposes. In this regard, you may like to refer to Section 27.9, Chapter 27. Business information could also be accessed by domestic government agencies or government agencies overseas – this may happen if the cloud provider retains the information outside of the country. For businesses that are thinking of going in a cloud service, it is important to understand the security and privacy policies and practices of the provider. The terms of service that govern the business relationships with the cloud service provider may allow for rather liberal usage and retention practices.

The Pros and Cons of Cloud Computing

In cloud computing scenario, very often, network security border is not fixed or well demarcated. As such, cloud computing implies loss of control! User may lose control even while being accountable – even if operational responsibility falls upon third parties; the 'Ifs' and 'Buts' and other critical terms need to be very thoroughly defined in the contract with cloud service provider organizations. Moreover, the security duties of (cloud service) provider and user differ greatly depending on the cloud model in use.

The growing popularity of cloud computing and virtualization among organizations have made it possibly the next target of cybercriminals. Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which makes it easier for cybercriminals to attack these systems. It all sounds great but there are pros and cons with cloud computing also. Although cloud computing does provide some benefits, it brings forth privacy and security concerns too. After all, under the cloud paradigm, your precious data is travelling over the Internet and is stored on servers in remote locations. In addition, the risks could emerge from the operational practice followed by cloud providers – often the providers serve multiple customers simultaneously and that too from the same domain, that is, financial industry, healthcare domain where personal data privacy is very high. All these factors combined may push up the scale of exposure to possible breaches, accidental as well as deliberate, as the case may be.

Many have raised the concerns that cloud computing may lead to 'function creep' meaning that uses of data by cloud providers that were not anticipated when the information was originally collected and for which consent has typically not been obtained. In this context, the IPPS in Section 27.9 of Chapter 27 are very important. Also refer to the Fair Information Practices (the FIPs) explained in Section 27.8 of Chapter 27. Given that it does not cost so much to keep data with cloud service providers, there is a growing tendency to leave more and more information in the cloud and therefore, in turn, some interested parties have more reasons to invent other things to do with it! (e.g., leak of personal information such as the credit card data, health information etc.). Thus, the world of cloud computing is not free of risks; these risks come mainly from security and privacy perspective.

BOX 7.10

Cloud and Data 'Ownership'

There are some philosophical questions regarding cloud computing; some of them pertain to 'data ownership'. For example, a fair question is 'Does the user or company subscribing to the cloud computing service "own" the data?' Or 'Does the cloud computing system, which provides the actual storage space, own it?' Or 'Is it possible for a cloud computing company to deny a client access to that client's data?' Several companies, law firms and universities are debating these and other questions about the nature of cloud computing. Data ownership issues in cloud computing can be thorny legal issues for sure.

Is cloud computing likely to affect industries other than those in the financial domain? The concern is rising in the IT industry as to how cloud computing could impact the business of computer maintenance and repair. If companies adapt to the usage of streamlined computer systems, they may have fewer IT needs. According to some experts, the need for IT jobs will migrate to the back end of the cloud computing system.

BOX 7.10 (Continued)

Autonomic computing is another hot area of research in the computer science community. An autonomic computing system is self-managing, which means the system monitors itself and takes measures to prevent or repair problems (in this connection it is useful to recall the discussion about intelligent software agents and related privacy issues (refer to Section 28.76, Chapter 28).

As things stand now, autonomic computing is mostly theoretical. However, in the near future, if autonomic computing becomes a reality, it could eliminate the need for many IT maintenance jobs.

In the reference section at the end a few links are provided to reading material in this area.

Fair Information Practices (the FIPs) and Information Privacy Principles (IPPs)

There are 8 FIPs and 11 IPPs. **Refer to Sections 27.8 and 27.9 of Chapter 27.**

Security Issues in Cloud Computing Models

In Table 7.2 categories of cloud computing technology were presented. They are essentially the various models of implementation. As explained in that table, IaaS() is the cloud computing model in which a pool of resources, such as servers, storage, networks, and other computing resources, is provided in the form of virtualized systems, which are accessed through the Internet. Users are allowed to run any software with full control and management on the computing resources allocated to them for use. Under the IaaS model, the users' cloud server has better control over the security compared to the other models only if there is no weakness in the security of the virtual machine monitor. Users control the software running in their virtual machines, and they are responsible for the correct configuration of security policies. However, the primary infrastructure (for computing, establishing the network, and data storage) is controlled by cloud service providers. As such, IaaS providers must expend a substantial effort to secure their systems to minimize these threats arising from creation, communication, monitoring, modification and mobility of the data.

BOX 7.11

Server Virtualization

Many people tend to associate *server virtualization* exclusively with cloud computing; however the concept of server virtualization is not new; it has been an important aspect of the IT (information technology) world for more than 30 years. In the days when the price of computing hardware was high and when the hardware continued to be important (even with falling hardware), sharing hardware capability among various applications became essential – the number of servers in use was increasing exponentially. In the recent years, server virtualization continues to be one of the key trends in IT as a way to cut costs, to become more energy efficient, and to reduce IT complexity.

Server virtualization is simply the partitioning of a physical server into smaller 'virtual servers' with a view to maximize server resources. The basic idea in server virtualization is to hide or mask the computing resources of the server from users. The number and identity of processors, operating systems and individual physical servers, etc. is hidden from the users of the given server. Special software is used to divide the physical server into multiple virtual environments; each is called virtual or private servers. This is in contrast to the concept of dedicated server in which one server is dedicated to a single application or task.

Thus, while there are various types of schemes for virtualization, all of them share one thing in common – the end result is a virtualized simulation of a computing resource or of a hardware device. Virtualization is typically achieved by partitioning a single piece of hardware into two or more 'segments and each segment operate as its own independent environment. In order to divide one physical server into multiple instances of isolated virtual environment, the server administrator uses a special software application. 'Virtual private servers' is the term may be used to denote these *virtual environments* – alternatively, they may also be denoted by terms such 'guests', 'instances', 'containers' or 'emulations'. Server virtualization can be achieved through more than one approach and the three methods mentioned here are considered to be popular: (1) the virtual machine model, (2) the para-virtual machine model, and (3) virtualization at the operating system (OS) layer. However, a detailed discussion on each of these is beyond the scope of the chapter; the reference section has additional links on the topic.

Some of the security issues (associated with IaaS, SaaS, PaaS) are presented below:

While virtualization allows users to create, copy, share, migrate and roll back virtual machines, which may allow them to run a variety of applications, it also provides new opportunities for cyber attackers. This is because of the extra layer that must be secured, for example, the VM (Virtual Machine – see Box 7.11). Security of the VM becomes as important as the security of the physical machine because any flaw in either one may impact the other. In normal infrastructures, virtualized environments are susceptible to all kinds of cyberattacks and as such, security is a greater challenge given that virtualization brings in additional points of entry and a greater complexity of interconnections. VMs have two boundaries: physical and virtual which is unlike physical servers.

There are security issues with SaaS (Software-as-a-service) too. As mentioned in Table 7.2, SaaS provides application services on demand – these are services such as conferencing software electronic mail systems as well as business applications such as ERP (enterprise resource planning), CRM (customer relationship management) and SCM (supply chain management). As compared to the three fundamental delivery models in the cloud, SaaS users have less control over security. Therefore, adoption of SaaS applications may raise some security concerns, especially from the perspective of application security. Under the SaaS model of cloud deployment, software applications are delivered via the Internet through a Web browser. Defects in web applications may create vulnerabilities for SaaS applications. The Web is the favorite place for cyber attackers to realize their objective of compromising user's computers and perform malicious activities such as steal sensitive data.

Recommended reading: Chapter 2 (Cyber Offenses: How Criminals Plan Them) of author's book titled '*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*', Wiley India, isbn: 978-81-265-2179-1.

Security challenges in software applications, delivered through the SaaS model of cloud, are basically the same as those that exist in any web application technology. However, traditional security solutions do not provide adequate protection against web-based attacks and therefore, new approaches become essential. The 10 top most security threats for web applications have been identified by the Open Web Application Security Project (OWASP). It is a good idea to start with securing web applications while there are many more security issues. When hackers access applications over the Internet via web browser, it makes it easy for them to access them (i.e. the applications) from any network device, which includes not only mobile devices but also public computers (as for example in the case of public cloud – illustrated in Figure 7.6).

Recommended reading: Chapter 3 (Cybercrime Mobile and Wireless Devices) of author's book titled '*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*', Wiley India, isbn: 978-81-265-2179-1.

At the same time, it also exposes the cloud service to additional security risks. The Cloud Security Alliance has released a report about the current state of mobile computing – it talks about the top threats in this area such as insecure networks such as the WiFi, that is, wireless networks, mobile malware to steal information from mobile devices, OS vulnerabilities in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

The PaaS (*Platform-as-a-Service*) models are used to achieve deployment of cloud-based applications without incurring the cost of buying and maintaining the underlying hardware and software layers. As with SaaS and IaaS models, the PaaS model also depends on a reliable and secure network along with secure web browser. There are two software layers involved in application security of PaaS: (1) security of the PaaS platform itself (i.e., runtime engine) and (2) the security of customer applications deployed on a PaaS platform. PaaS providers' responsibility lies in securing the platform software stack in which there is the runtime engine for running customers' software applications. As is the case with the SaaS model, the PaaS model of cloud also presents data security issues and related challenges – briefly described below. As we can see, they revolve around three major factors: (1) vendor relationships, (2) SDLC (software development life cycle) related security and (3) security of the IT infrastructure. Let us understand each of these three.

1. **Third-party relationships:** PaaS provides traditional programming languages, as well as third-party web services components. These components combine more than one source element into a single integrated unit. Therefore, the PaaS model of cloud implementation also inherits security issues related such as data security and network security. Moreover, PaaS users are dependent on both aspects of security, that is, the security of web-hosted development tools as well as the security of third-party services.

2. The SDLC related factors: From the perspective of application development, software developers are often challenged with the complexity of building secure applications that may be hosted in the cloud – in this regard the discussion in Section 26.16 of Chapter 26 is very important. In the cloud, rapid changes are made to the software applications developed for business enterprises and these changes do impact the System Development Life Cycle (SDLC) as well as security. As such, developers must be mindful of the fact that PaaS applications should be upgraded frequently, so they need to ensure that their application development processes are flexible enough to keep up with changes. That is how the trend towards Agile Software Development has emerged. It is important for the developers to understand that any changes in PaaS components can impact the security of their applications. In addition to the use of techniques for secure software development (refer to Section 26.16, Chapter 26), developers also need to get educated about legal issues in data management , to make them aware that data should not be stored at inappropriate locations. This is crucial because clients' data may be stored at different locations with different legal regimes that can compromise its privacy and security.

BOX 7.12

Agile and SCRUM in Cloud Context

Agile development model is one of the models classified under the broad class of life cycles called 'Iterative-Incremental Development Models'. 'Agile' is term associated with athletes and we know that it reminds of something that is exactly opposite of rigid or laborious. 'Agile' reminds us of something that is 'on-the-fly'. Agile methods in software became popular due to their promise to accommodate change and deliver rapidly with regard to the expectations of business. Agile methods are 'lightweight', that is, smaller teams and less documentation are emphasized rather than process paraphernalia and complex teams). Agility aspires to deliver immediate value to business. People, their skills and motivation, and their intra- and intergroup communications remain fundamental to the success of the agile approach – see Figure 7.9. 'Agile' values PEOPLE more than PROCESSES.

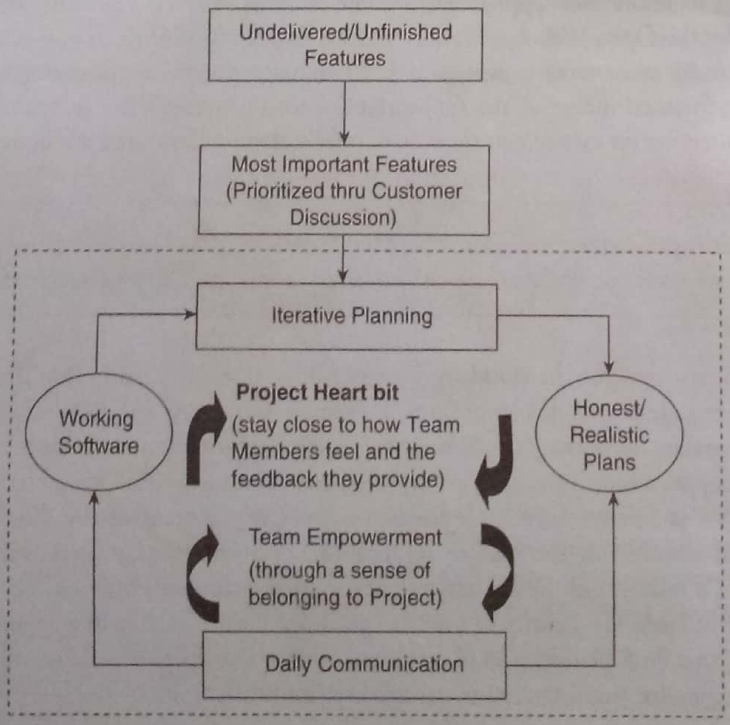


FIGURE 7.9 | Agile methodology.

'Agile' uses SCRUM as a process to allow developers to focus on delivering the highest business value in the shortest time. The 'SCRUM' technique was introduced in 1996 at OOPSLA conference. SCRUM allows teams to rapidly and repeatedly inspect actual working software (every two weeks to one month). In AGILE, the business and its users set the priorities. Agile teams self-manage to determine the best way to deliver the highest priority features. In a short period of time, real working software can be seen and a decision about its release can be made or it can be decided to continue to enhance for iteration.

3. **Security of the underlying infrastructure:** In PaaS, software developers do not generally have access to the underlying layers. Therefore, cloud service providers have the responsibility of securing the underlying IT infrastructure as well as the applications services. Software developers working in PaaS paradigm do not have the assurance that the development environment tools provided by a PaaS provider are secure. This is so even when developers are supposed to control the security of their applications.

Cybercrime on Cloud Nine! – Protecting Data Privacy and Information Security in the Cloud

Security is of utmost importance. However, often, cybercrime takes place due to poor security protocols and unavailability of an IT support that many businesses and individuals cannot afford. Weak wireless passwords and unencrypted online data storage without adequate security precautions offer the biggest threats to online security. People expect that the technological progress of cloud computing offers a viable solution to these security vulnerabilities. Cloud computing is usually looked upon as a challenge to the global regulation of the Internet. In the domain of information security, data privacy concerns involve questions of IT infrastructure protection and the fight against crime, along with the defense considerations linked with possibilities of cyber-spying and cyber-sabotage. Table 7.3 lists the major areas of concerns in cloud computing domain.

TABLE 7.3 | Major areas of concerns in cloud computing domain

Sr. no	Area	What is the risk?	How to remediate the Risk?
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendor's monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.
4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster – availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.
6.	Information security violation reports	Due to complex IT environment and several customers logging in and logging out of hosts, it becomes difficult to trace inappropriate and/or illegal activity.	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
7.	Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.	Organization should ensure getting their data in case of such major events.

Source: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (9 October 2009).

We ought to keep in mind that 'Clouds' are not single point servers; they rely on a network of encrypted servers that are configured to distribute information across wide geographic areas where the networks operate. With larger and larger organizations and professionally managed web-networks, we can be assured of a strong architecture that reduces the threat posed by cyber hackers. One benefit of such a system is the removal of information from fixed points – for example, localized networks and individual computers. It effectively eliminates vulnerable access points to data storage and provides protection against un-authorized or unofficial software installation.

Depending on the types of information distribution, cloud networks can get exposed to prolonged attacks that exploit weak points in network security. There is a famous saying that security is as strong as the weak link in the security chain; therefore, even if one server has weak defense, it may result easy access to other localities in the network. Many governments consider Internet regulation as the panacea to online security issues; that however, does not work in the intended manner. There is now a greater industry consensus to stand firmly against cyber criminals. As mentioned in Section 7.6, data ownership, access and security protocols (depending on the location of servers) are important aspects to focus on while signing contracts with cloud service providers. The implementation of standardized protocols would further improve security for weaker systems to deter cyber attacks on cloud systems. The haunting question, in the face of our growing dependence on cloud-based computing, is whether cloud computing can prevent cybercrime? Many organizations are still not so ready to trust third-party storage and apparently, there is no evidence to support the idea that dedicated cloud-based security is a step in the right direction.

To conduct highly automated online banking theft, cyber criminals use the same flexibility and freedom that business organizations enjoy from having their software and services hosted in the cloud. When the victim logs into the bank site, the malware would use a so-called Web inject technique to overlay what looks like the bank Web page in the victim's browser. Behind the scenes however and not at all known to the victim, something very different is happening. While the victim is under the impression that he or she is transferring money from his/her savings account into another of his/her account, for instance, the malware is actually transferring any amount of money to the account that has been specified by the cyber criminals! Most often these are cyber criminals' own accounts!

A number of scenarios like the one mentioned above are addressed in case studies in author's book titled '*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*', Wiley India, isbn: 978-81-265-2179-1.

As a traditional practice, banking malware like this will handle the processing from the victim's PC. But these days, it is being noted that the heavy lifting of the malware is being done on the server in the cloud – the servers are located mostly at an ISP (Internet Service Provider) with not so strong security policies and the location of the servers is changed frequently to avoid discovery. However, more than this what is required is 'strong authentication'.

Refer to Section 11.2 of Chapter 11: Biometrics for Security to know about **Access Control, User Identification and User Authentication.**

Recommended reading: Section 2.4.1 of Chapter 2 (Cyber offenses: How Criminals Plan Them), of author's book titled '*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*', Wiley India, isbn: 978-81-265-2179-1.

Criminals go to the extent of bypassing even the two-factor authentication systems that are commonly used in most online banking systems – the consumer is required not only to type in a username and password to an online banking site, but also has to swipe a card into a special card reader attached to the PC that provides additional data proof that the legitimate user is accessing the account. There a 'multi-factor authentication' system is considered much stronger (from cyber-attack perspective) which is a combination of three factors: (1) what you know, (2) what you have and (3) what you are (biometrics). As mentioned in the discussion so far, a prime area of the risk in cloud computing is the protection of user data. According to a recent study, one of the main risks that comes due to the growing dependence on cloud computing is not as much as the increase in cyber fraud or crime than the loss of control over individual identity and data. Phenomenon such as 'cyber stalking' are on rise resulting in a growing feeling among individuals as if they were being watched – refer to 'data surveillance' mentioned in Section 28.2 of Chapter 28 (Privacy – Business Challenges and Technological Impacts).

Thus, while there are serious security risks, but with the right type of protective measures established, they could be minimized or overcome to some extent. It is true that the challenge relates to the protection of citizens against crime, and to guarantee their fundamental freedoms and rights in the context of an increasingly cloud-intensive Internet.

Many studies conducted during the recent years indicate that even with cloud computing, cybercrime is not particularly singled out as a specific concern. Among the 10 'top security risks' listed by such studies on the cloud, there are only two or three concerns that are potentially related to criminal activities. They point to the possibility of attacks launched on isolation mechanisms, given that cloud computing bases itself on multi-tenancy and is a model based on shared resources. The compromising of management interfaces could give attackers access to a potentially greater set of resources than in traditional, networked computing, and the possibility of a 'malicious insider' lurking within the organization of the cloud service provider. These risks could possibly have something to do with the overlooking of traditional information security measures rather than something brought about exclusively by cloud computing.

Cyber Stalking

Recommended reading: Section 2.4.1 of Chapter 2 (Cyber Offenses: How Criminals Plan Them) of author's book titled '*Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*', Wiley India, isbn: 978-81-265-2179-1.

7.7 Protecting Information Security and Data Privacy in Cloud Computing

In a mobile computing environment, clients can virtually log in from any location to access data and applications. In such a scenario, client's data privacy could be compromised. Therefore, organizations that provide cloud computing services need to find ways to safeguard client data privacy. There is one way to achieve this through the use *authentication techniques* such as user names and passwords [for greater details of this, refer to Section 12.3, Chapter 12 and Box 32.4, Chapter 32]. Another is to employ an *authorization format* – each user can access only the data and applications relevant to his or her job, that is, business need based access management.

BOX 7.13

PIPEDA and Cloud Data Privacy

'Data Privacy' can become a maker–breaker situation, that is, a barrier in the implementation of cloud-based services and therefore, it must be taken into consideration. The European Union (EU) has a strong EU clause for the protection of business *data privacy protection*. The EU Data Protection Directive mandates the consent of the data subject to process their personal data in accordance with the 'purpose of collection' (in this regard, you may like to refer to 'Information Privacy Principles' – the IPPS in Section 27.9, Chapter 27). The *data subject* is usually an individual; however, depending on the business proceedings, data subject can also be a corporate entity. 'Personal data' includes data such as email address, business contact details and other information attributable to an individual. The data is collected and controlled under terms agreed with the data subject; for example, an employment agreement, agreements made by works council, privacy policy, customer agreement or consent over telephone. The EU Data Protection Directive gives the data subject right to project data privacy.

PIPEDA stands for *Personal Information Protection and Electronic Documents Act*. In Canada, *PIPEDA* is the privacy legislation in private sectors that governs the collection, use and disclosure of personal information in the course of commercial activity. PIPEDA applies to organizations in the private sector, as well as federal works and undertakings (such as banks and airlines). *PIPEDA* defines personal information to broadly encompass almost any information that can be attributed to an *identifiable individual* (in regard to this concept, refer to Figure 27.1 and Figure 27.2 of Chapter 27 – Privacy: Fundamental Concepts and Principles). The meaning of 'personal information' within the context of *PIPEDA* can have a ...very elastic definition and it ought to be interpreted in that way to make the purpose of *PIPEDA* meaningful. The purpose of the Act, that is, PIPEDA, is to recognize *the right to individual privacy* in a technological era that increasingly facilitates the exchange of information, by imposing obligations on organizations with access to individuals' personal information. *PIPEDA* applies to all Canadian provinces and territories, with a few exceptions, whose discussion is not warranted within the scope of this chapter.

To gain greater understanding about the legal implications of data privacy breaches, we recommend reading of Chapter 6 (Cybercrimes and Cybersecurity: The Legal Perspectives), of author's book titled **'Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives'**, Wiley India, isbn: 978-81-265-2179-1.

It is important to keep in mind that policies and legal acts are good measures; however, often they work only as deterrent to fraud and not as a complete stoppage. In the same way, the Personal Information Protection and Electronic Documents Act (PIPEDA)

does not prevent an organization from transferring personal information to an organization in another jurisdiction for the purpose of data processing. PIPEDA does, however, establish certain rules for governing those data transfers — particularly with respect to obtaining consent for the collection, use and disclosure of personal information, securing the data, and ensuring accountability for the information and transparency in terms of practices. Given the spread of digital IT assets, distributed computing, remote access and the global economy with its increasing dependence on information assets residing in the virtual (cyber) space, there are enormous challenges, especially in the domain of financial and healthcare organizations (in this regard, also refer to Section 40.5 of Chapter 40), when it comes to protecting data privacy of clients. The completion discussion on this is beyond the scope of this chapter; interested readers may like to refer to articles and papers noted at the URLs provided at the end of the chapter.

Equally important is to identify, implement processes and security controls to maintain effective governance, risk management and compliance. In the contract phase, (cloud service) provider security governance should be assessed for adequacy, maturity, consistency with the standards that are acceptable to the user, that is, the organization that takes the cloud service. Some of the *best practices* worth mentioning in this regard are: requesting clarity on how cloud service provider's facility and services will assessed by the user organization before signing the contract, requiring a clear definition of what the provider considers 'critical services', performing full contract, terms of use, due diligence to determine roles, responsibilities and accountability of both parties involved in the contract for cloud services. It is good to include the 'right to audit clause' clause so that provider's IT facilities can be inspected with or without prior notice as per agreed terms in the contract. It is good to analyze compliance scope as well as regulatory impact on data security. End-user organization should ensure that 'evidence requirements' are met – for this it is best to base the operational audits on some world-class standards such as the ISO 27001.

Refer to: **Chapter 23: ISO 17799/ISO 27001**

You may also like to refer to:

Section 27.9 - Information Privacy Principles (IPPs)

Table 27.1 - Information Privacy Principles (List) and their explanation in Chapter 27.

People wonder if cloud computing may improve privacy protection. For businesses that are planning to go for a cloud service, in author's opinion, it is myth to believe that cloud computing could offer better protection of personal information compared with current security and privacy practices. However, it is fair to believe that using the economies of scale, large cloud providers may be in a position to deploy better security technologies than individuals or small companies can, and thus, they may have better backup and disaster-recovery capabilities (you may like to refer to Chapter 31 to consult the fundamentals of BCP and DRP).

Cloud providers' motivation may also be to build adequate privacy protections into new technology, and to support better audit trails. At the same time, even though cloud computing may not heighten the risk of improper exposure and misuse of personal information, it could increase the scale of exposure. The storing of business-sensitive data in a cloud service provider's site can make that data an attractive prey to cybercriminals, for example. Moreover, given that these days it does not cost so much to keep data in the cloud, there may be a tendency to retain it indefinitely, and thus increasing the risk of data breaches which often invoke penalties and legal implications. In view of this, some of the good practice recommendations are: ensuring that all data copies and backups are stored only at location allowed by contract, strictly monitoring the SLA (refer to Box 7.6 - SLA and SLO) and/or all applicable regulations (e.g., the PIPEDA – refer to Box 7.13). Given the sensitivity of data in the healthcare sector, data storage practices need to be compliant with prescribed standards for data protection. In case you change your cloud service provider, areas to watch are: change in contract price, financial strength of the cloud service provider, possibilities of provider service shutdown, degradation in the service quality of the cloud service provider, potential areas for business disputes between you and your service provider. In addition to these precautions, one should not overlook the possibilities of 'insider threat' from within the (cloud service) provider's organization. Therefore, as mentioned earlier, a good idea is to maintain the right for the user organization to carry onsite inspections of provider's IT facilities including provider's documented and tested plan for disaster recovery, business continuity, etc. (for details refer to Chapter 31).

Ensuring that the service provider has 'measurements and metrics place' is another good idea (refer to Chapter 25). Typically such metrics (for ensuring good service from providers) are: on-demand self-service, broad network access, IT resource pooling, rapid elasticity (see Box 7.6), service measurability based on mutually agreed parameters. Another important aspect to keep in mind in regard to security with cloud services is that cloud applications are not always designed with data integrity and security in mind. Therefore, it is absolutely essential to ensure that the service provider has firewall and IDS (intrusion detection service) logs in place. Provider must also deliver snapshots of end-user's virtual environment. All the sensitive data must be encrypted for getting protection against data breach regulations.

Encryption, Intrusion Detection and Firewalls

Recommended reading (from this book):

Chapter 14: Cryptography and Encryption
Chapter 15: Intrusion Detection for Securing Networks
Chapter 16: Firewalls for Network Protection

Legal implications of data privacy breaches

Recommended reading: Chapter 6 (Cybercrimes and Cybersecurity: The Legal Perspectives) of author's book titled 'Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives', Wiley India, isbn: 978-81-265-2179-1.

As far as identity management and access management are concerned, it must be determined how the cloud service provider handles provisioning, de-provisioning of IT resources, authentication and authorization, federation and user profile management (for the concept of 'federation', refer to Chapter 29, in particular to Box 29.1 – federated identity, federated trust management and federated networks in that chapter). Server virtualization is explained in Section 7.5.2 (Box 7.10): in that context, from a security control perspective, the client organization must determine the type of virtualization used by the provider, the third-party security technology augments the virtual OS (operating system) and the controls used by the cloud service provider to protect admin interfaces that are exposed to users. Often the weakness lies in the OS that is not hardened (refer to Chapter 21). To summarize and close the discussion on security measures in cloud, Figure 7.10 presents a model for performing the gap analysis (for security controls) by analyzing the various requirements (as presented in the figure) for selecting an appropriate cloud service provider.

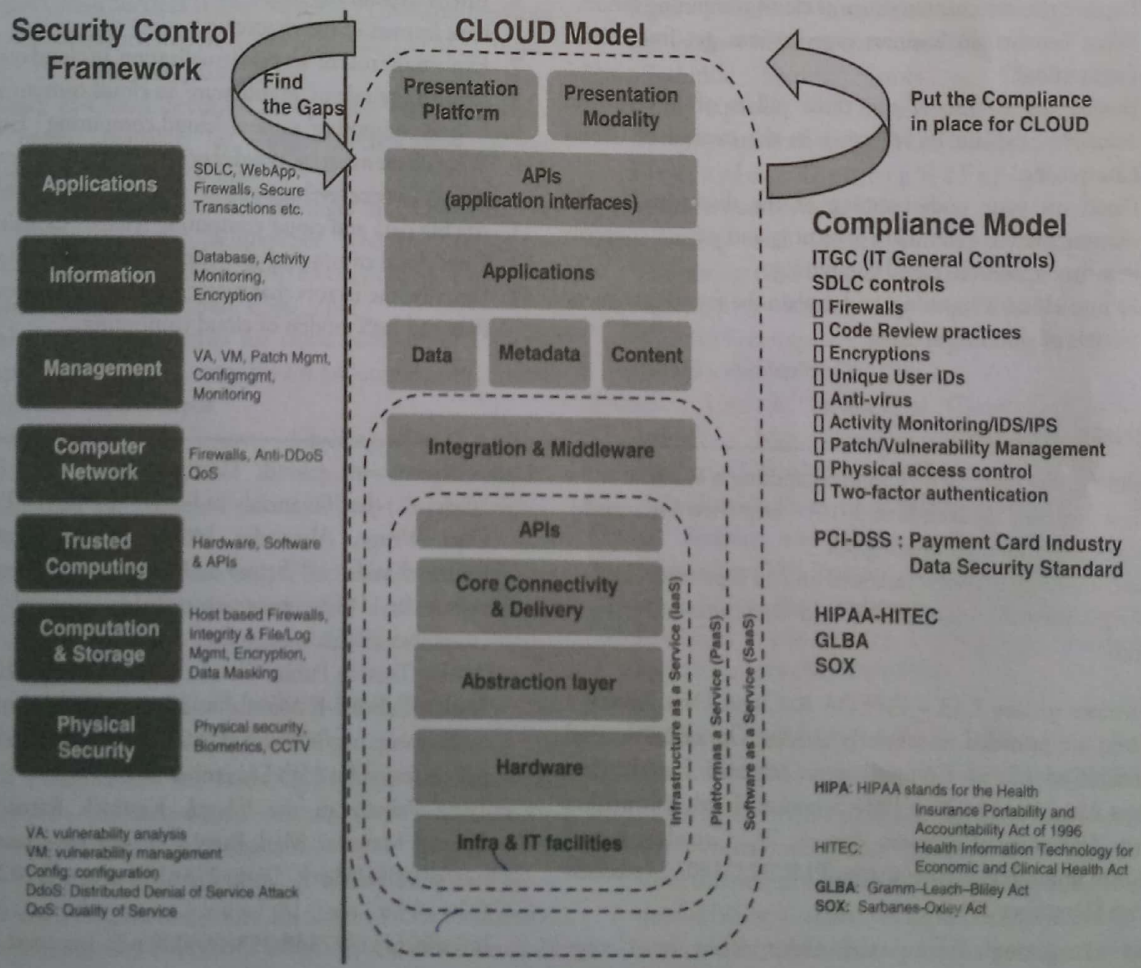


FIGURE 7.10 | Gap analysis for cloud security.

For the details of elements shown in Figure 7.10, that is, physical security and biometrics, refer to Chapter 7 and Chapter 11, respectively.

Summary

Cloud computing is simply the delivery of computing services over the Internet. Cloud computing enhances collaboration, agility, scalability, availability and ability to adapt to fluctuations according to demand, accelerate development work, and provide potential for cost reduction through optimized and efficient computing. There is no doubt about the growing importance of cloud computing; therefore, it is not a surprise that the area is receiving a growing attention in the scientific as well as industrial communities. Cloud computing is considered as one of the top 10 most important technologies. Cloud services are popular because they provide a convenient way for people to access their e-mail, social networking site or photo service from anywhere, anytime across the globe, and at minimal or no charge. However, on the down side, some cloud providers may, however, use the personal information of users for advertising purposes or to learn more about the users for other reasons. Cloud computing combines existing techniques and technologies and packs them within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs and just-in-time availability of resources – these are some of the features that we presented in the chapter. Organizations are interested in cloud computing because with cloud computing they can significantly reduce the cost and complexity of owning and operating computers and networks. An organization that uses a cloud provider saves money because it no longer needs to spend money on the IT infrastructure or buy hardware or software licenses. The flexibility of cloud services makes it possible to get them customized to users' specific computing needs, and providers can offer advanced services that an individual company might not have the money or expertise to develop. In this chapter we learned about cloud computing characteristics and some of the key security and privacy issues involved in the use of the cloud technology.

Review Questions

1. Explain the key characteristics of cloud computing model.
2. What benefits do business organizations get from cloud Computing?
3. *Availability* is one of the three pillars of information security – explain its relevance in the context of Cloud Computing.
4. Based on your understanding of the discussion in the chapter, present a summary of security and privacy concerns that may arise from cloud computing.
5. Define 'cloud computing' and explain the four deployment models of cloud computing.
6. Briefly explain the major 'service models' of cloud that you have learned in the chapter.
7. Explain the role of 'server virtualization' in cloud computing.
8. Explain the role of 'middleware' in cloud computing.
9. Is 'grid computing' same as 'cloud computing'? Explain.
10. What do we mean by 'cloud elasticity'? Explain the importance of SLA (service level agreement) in cloud service contracts.
11. Are big data and cloud computing related? Explain how.
12. Does cloud computing give rise to 'data ownership' issues?
13. Describe the factors that may create security issues in SaaS, Paas and IaaS models of cloud computing.

Further Reading

A useful reading material on Cloud computing is available at the link (accessed on 26th June 2010) – http://www.qsarworld.com/files/Cloud-computing.pdf

Cloud computing overview (accessed on 2nd September 2012) – http://www.thbs.com/pdfs/Cloud-Computing-Overview.pdf

In reference to Box 7.13 – PIPEDA & Cloud Data Privacy, a few links are provided to scholarly articles: Opportunities and Challenges of Cloud Computing to Improve Health Care Services, Alex Mu-Hsing Kuo, PhD, School of Health Information Science, University of Victoria, Victoria, BC, Canada – http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/ (accessed on 15th December 2015).

Cloud Computing: Privacy and Other Risks by George Waggott, Michael Reid and Mitch Koczerginski, McMillan LLP is available at the URL (accessed on15th December 2015): http://www.mcmillan.ca/Files/166506_Cloud%20Computing.pdf

Data Privacy in Cloud Computing – An Empirical Study in the Financial Industry (Research Paper) by Olga Wenge, Alexander Müller, Ulrich Lampe, Ralf Schaarschmidt at http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1166&context=amcis2014 (accessed on 15th December 2015).

Establishing Trust in Public Clouds, Jogesh K Muppala, Deepak Shukla, Subrota K Mondal and Pranit Patil at http://www.omicsgroup.org/journals/2165-7866/2165-7866-2-e107.pdf (accessed on 15th December 2015).

Clarifying Privacy in the Cloud, Karthick Ramachandran, Thomas Margoni, Mark Perry at https://www.researchgate.net/profile/Mark_Perry2/publication/228204627_Clarifying_Privacy_in_the_Clouds/links/0fcfd510773dfb253e000000.pdf (accessed on 15th December 2015).

Data Security – The Case Against Cloud Computing (Canadian Privacy Law Review) at http://www.casselsbrock.com/files/file/B%20Karn%20Cloud%20

Security of Wireless Networks

9

Learning Objectives

After completing this chapter you will be able to:

- obtain an overview of wireless technology.
- understand the scenario of wireless network technology usage.
- learn about wireless technology in security context.
- learn about attacks on wireless networks and the risks arising from the attacks.
- understand the need for countermeasures to mitigate security risks.

9.1 Introduction

Wireless technologies have become increasingly popular in our everyday business and personal lives. Handheld devices such as the personal digital assistants (PDAs) allow individuals to access calendars, electronic mail (e-mail) addresses and phone number lists and the Internet. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs. Wireless networks are generally composed of two basic elements: access points (APs) and other wireless-enabled devices, such as laptops (see Figure 9.1). Both of these elements rely on radio transmitters and receivers to communicate or 'connect' with each other. APs are physically wired to a conventional network, and they broadcast signals with which a wireless device can connect.

Readers should recall that in Chapter 6, information security (InfoSec) issues in mobile and wireless computing paradigms were discussed. This chapter will touch base with those concepts only as a passing reference. The focus of this chapter is the security and vulnerability issues with wireless networks. We start this chapter by examining some basic terms relating to the world of wireless. The first basic term to be introduced is 'Wi-Fi' (wireless fidelity, recall Box 17.2 in Chapter 17 that explained what a 'Wi-Fi AP' is). The term is promulgated by the Wi-Fi Alliance. Any products tested and approved as 'Wi-Fi Certified' (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a 'Wi-Fi Certified' product can use any brand of AP with any other brand of client hardware that also is certified. We build upon these ideas and discuss the role of wireless networks in today's paradigm. Wireless networks are also referred to as Wi-Fi or 802.11 networks. They use a radio link instead of cables to connect computers. Wireless security can be broken into two parts: authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an AP and vice versa, while encryption mechanisms ensure that it is not possible to intercept and decode data.

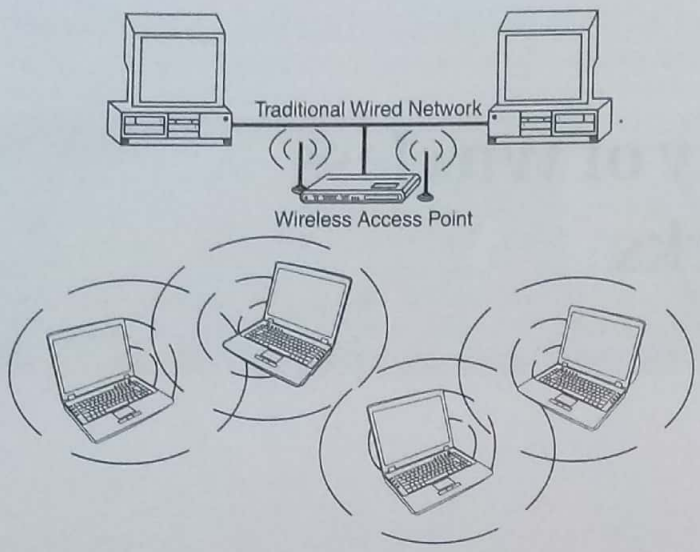


FIGURE 9.1 | An example of a wireless infrastructure mode network.

Courtesy: GAO, May 2005 report on Information Security, titled Federal Agencies Need to Improve Controls over Wireless Networks. GAO is United States Government Accountability Office.

9.2 An Overview of Wireless Technology

In the simplest sense, wireless technologies enable one or more devices to communicate without physical connections, that is, without requiring a network or peripheral cabling (see Figure 9.1). Wireless technologies use *radio frequency* (RF) *transmissions* as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems such as *wireless local area networks* (WLANs) and cell phones to simple devices such as wireless headphones, microphones and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. In the *wireless technologies* arena, the important ones are: wireless networks (WLANs and ad hoc networks), wireless devices (PDAs and smart phones – recall the discussion in Chapter 6) and the wireless standards for communication. A brief overview of wireless networks, devices, standards and security issues is presented as follows:

1. **WLANs:** They allow greater flexibility and portability than do traditional wired local area networks (LANs). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an AP device. Users move freely within the cell with their laptop or other network device. AP cells can be linked together to allow users to even 'roam' within a building or between buildings.
2. **Ad hoc networks:** Ad hoc networks such as *Bluetooth* (see Box 9.1) are networks designed to dynamically connect remote devices such as cell phones, laptops and PDAs. These networks are termed 'ad hoc' because of their shifting network topologies.

BOX 9.1

Bluetooth

Bluetooth is a short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers. Products with Bluetooth technology must be qualified and pass interoperability testing by the *Bluetooth Special Interest Group* (SIG) prior to release. The original architect for Bluetooth, named after the tenth century Danish king Harald Bluetooth, was Ericsson Mobile Communication.

BOX 9.1 (Continued)

In 1998, IBM, Intel, Nokia and Toshiba formed the *Bluetooth SIG*, which serves as the governing body of the specification. Bluetooth was originally designed primarily as a cable replacement protocol for wireless communications. So, the founding members of Bluetooth include Ericsson, IBM, Intel, Nokia and Toshiba. Today, Bluetooth has emerged as a very popular ad hoc network standard.

The Bluetooth standard is a computing and telecommunications (TC) industry specification that describes how mobile phones, computers and PDAs should interconnect with each other, with home and business phones and with computers using short-range wireless connections. Bluetooth network applications include wireless synchronization, e-mail/Internet/intranet access using local personal computer (PC) connections, hidden computing through automated applications and networking and applications that can be used for such devices as hands-free headsets and car kits.

The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 720 kbps. It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The Institute of Electrical and Electronics Engineers (IEEE) 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1. The plan is to develop a broad range of Bluetooth-enabled consumer devices to enhance wireless connectivity. Among the array of devices that are anticipated are cellular phones, PDAs, notebook computers, modems, cordless phones, pagers, laptop computers, cameras, Personal Computer Memory Card Industry Association (PCMCIA)-compliant cards, fax machines and printers. Bluetooth is now standardized within the IEEE 802.15 Personal Area Network (PAN) Working Group that was formed in early 1999.

Courtesy: http://www.webopedia.com/TERM/b/bluetooth.html (accessed 17 September 2006).

3. **PDAs:** Readers should refer to Chapter 6; PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. They offer applications such as office productivity, database applications, address books, schedulers and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer (PC). Newer versions allow users to download their e-mail and to connect to the Internet. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network.
4. **Smart phones:** Mobile wireless telephones, or cell phones, are telephones that have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a 'cell'. As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next. Today's cell phone is rapidly evolving to integration with PDAs, thus providing users with an increased wireless e-mail and Internet access. Mobile phones with information-processing and data networking capabilities are called 'smart phones'.
5. **Wireless standards:** Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. For this section, the discussion of wireless standards is limited to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 and the Bluetooth standard. WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth SIG (see Box 9.1). These standards are IEEE 802.11 and Bluetooth. A full discussion on them is not within the scope of this book.

9.3 Wireless Network Usage Scenario Today and Implications

Wireless access to networks has become very common by now, in India as well, for both organizations and individuals. Many laptop computers have wireless cards pre-installed for the buyer, for example, in India, such cards are provided by TATA Indicom, Reliance and AirTel. There are many hotels and equivalent establishments all over the world (including India) where the rooms are 'Wi-Fi enabled'. There is no denying that the ability to enter a network while on the move (working away from home or in other locations that are not routine office locations, working while in hotels, etc.) has great benefits (see Box 9.2 for some interesting facts).

BOX 9.2

Going Wi-Fi

Start with a laptop computer or other portable device that could benefit from Internet access. Make sure it is wireless. Look for Intel's Centrino sticker or any sign that Wi-Fi is built into the device. If not, you need an external Wi-Fi PCMCIA-compliant card. Find a public hotspot by searching store windows for stickers that say Wi-Fi Zone, T-Mobile HotSpot or anything indicating a wireless service. Boot up your laptop and log in. Or at home or at a hotel, get a Wi-Fi router and plug one end into your cable or digital subscriber line (DSL) modem. The router will broadcast the wireless Internet signal in your house, so you can sit on the couch and surf the Internet.

Although wireless technology is not new, it is now being used by families who need an easy way to share a fast Internet connection with two or more computers at home. It is helping almost anybody, that is, even the 'non-techies', to get Internet access while they buy their daily cup of coffee at a Wi-Fi coffeehouse. This kind of scene is now very common in most Indian metros, including some small cities too.

Cell phones have become indispensable for many who use them to keep track of family members or to call for help in an emergency. Wi-Fi is not there yet, but the idea of wireless Internet access on every corner is becoming a 24/7 possibility as more companies set up public hotspots. Like cell phones, Wi-Fi is not something you will use every minute, but it can be convenient when you need to check for an e-mail message or compare the price of a gift online.

Courtesy: http://www.ocregister.com/ocregister/healthscience/technology/wifiwatch/article_459262.php (accessed 9 September 2006).

While all this sounds very exciting, it is important to understand that wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into. They are known to use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and should stay up-to-date on any new risks that arise. Users of wireless equipment must be aware of these risks so as to take personal protective measures. As the wireless service technology is getting improved and falling within an easy reach of information technology (IT) as well as non-IT workers, the risks to users of wireless technology have increased exponentially (Box 9.3).

BOX 9.3

What Color is Your Hat in the Security World?

When Edward DeBono wrote his epoch making the book *The Six Thinking Hats*, little did he know that the hats would follow suit in other domains too!! Just read on to discover about the 'hats' in security world. And not just that, do be conscious to know if any of these hats are around you to jeopardize the security of your information assets on the network.

A **black hat** is also called a 'cracker' or 'dark side hacker'. Such a person is a malicious or criminal hacker (the term 'hacker' is mentioned in Chapter 12 – Box 12.2 and Chapter 15 – Box 15.3. Hacker activities are explained in Chapter 16; see Box 16.4). Typically, the term 'cracker' is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer jargon, the meaning of 'hacker' can be much broader. The name comes from the opposite of 'white hat hackers'.

A **white hat** hacker is considered as an **ethical hacker**. In the realm of IT, a 'white hat hacker' is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a 'white hat' generally focuses on securing IT systems, whereas a 'black hat' (the opposite) would like to break into them, so this sounds like the age-old game of thief and police.

A black hat will wish to secure his/her own machine, and a white hat might need to break into a black hat's machine in the course of an investigation. What exactly differentiates white hats and black hats is open to interpretation, but white hats tend to cite altruistic motivations. Usually a black hat is a person who uses his knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or to the manufacturer for correction. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, black hats may work to cause damage maliciously.

Interestingly, this is not all; in the security world, there are hats of other colors too. A **brown hat** hacker is one who thinks before acting or committing a malice or non-malice deed. A **grey hat** commonly refers to a hacker who releases information about any exploits or security holes s/he finds openly to the public. S/He does so without concern for how the information is used in the end (whether for patching or exploiting). Viva Edward DeBono!!

Courtesy: http://en.wikipedia.org/wiki/Black_hat (accessed 5 September 2006).

BOX 9.2

Going Wi-Fi

Start with a laptop computer or other portable device that could benefit from Internet access. Make sure it is wireless. Look for Intel's Centrino sticker or any sign that Wi-Fi is built into the device. If not, you need an external Wi-Fi PCMCIA-compliant card. Find a public hotspot by searching store windows for stickers that say Wi-Fi Zone, T-Mobile HotSpot or anything indicating a wireless service. Boot up your laptop and log in. Or at home or at a hotel, get a Wi-Fi router and plug one end into your cable or digital subscriber line (DSL) modem. The router will broadcast the wireless Internet signal in your house, so you can sit on the couch and surf the Internet.

Although wireless technology is not new, it is now being used by families who need an easy way to share a fast Internet connection with two or more computers at home. It is helping almost anybody, that is, even the 'non-techies', to get Internet access while they buy their daily cup of coffee at a Wi-Fi coffeehouse. This kind of scene is now very common in most Indian metros, including some small cities too.

Cell phones have become indispensable for many who use them to keep track of family members or to call for help in an emergency. Wi-Fi is not there yet, but the idea of wireless Internet access on every corner is becoming a 24/7 possibility as more companies set up public hotspots. Like cell phones, Wi-Fi is not something you will use every minute, but it can be convenient when you need to check for an e-mail message or compare the price of a gift online.

Courtesy: http://www.ocregister.com/ocregister/healthscience/technology/wifiwatch/article_459262.php (accessed 9 September 2006).

While all this sounds very exciting, it is important to understand that wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into. They are known to use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and should stay up-to-date on any new risks that arise. Users of wireless equipment must be aware of these risks so as to take personal protective measures. As the wireless service technology is getting improved and falling within an easy reach of information technology (IT) as well as non-IT workers, the risks to users of wireless technology have increased exponentially (Box 9.3).

BOX 9.3

What Color is Your Hat in the Security World?

When Edward DeBono wrote his epoch making the book *The Six Thinking Hats*, little did he know that the hats would follow suit in other domains too!! Just read on to discover about the 'hats' in security world. And not just that, do be conscious to know if any of these hats are around you to jeopardize the security of your information assets on the network.

A **black hat** is also called a 'cracker' or 'dark side hacker'. Such a person is a malicious or criminal hacker (the term 'hacker' is mentioned in Chapter 12 – Box 12.2 and Chapter 15 – Box 15.3. Hacker activities are explained in Chapter 16; see Box 16.4)). Typically, the term 'cracker' is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer jargon, the meaning of 'hacker' can be much broader. The name comes from the opposite of 'white hat hackers'.

A **white hat** hacker is considered as an **ethical hacker**. In the realm of IT, a 'white hat hacker' is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a 'white hat' generally focuses on securing IT systems, whereas a 'black hat' (the opposite) would like to break into them, so this sounds like the age-old game of thief and police.

A black hat will wish to secure his/her own machine, and a white hat might need to break into a black hat's machine in the course of an investigation. What exactly differentiates white hats and black hats is open to interpretation, but white hats tend to cite altruistic motivations. Usually a black hat is a person who uses his knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or to the manufacturer for correction. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, black hats may work to cause damage maliciously.

Interestingly, this is not all; in the security world, there are hats of other colors too. A **brown hat** hacker is one who thinks before acting or committing a malice or non-malice deed. A **grey hat** commonly refers to a hacker who releases information about any exploits or security holes s/he finds openly to the public. S/He does so without concern for how the information is used in the end (whether for patching or exploiting). Viva Edward DeBono!!

Courtesy: http://en.wikipedia.org/wiki/Black_hat (accessed 5 September 2006).

There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. Currently, however, there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the IT department to keep up-to-date with the types of threats and appropriate countermeasures to deploy. Security threats are growing in the wireless arena. Crackers have learned that there is much vulnerability in the current wireless protocols, encryption methods and the carelessness and ignorance that exist at the user and corporate IT levels. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has become much easier and more accessible with easy-to-use Windows- and Linux-based tools being made available on the web at no charge. In the face of all this, IT personnel should be familiar with what these tools can do and how to counteract the cracking that stems from them.

9.4 Wired World versus Wireless World: Putting Wireless Networks in Information Security Context

Since wireless networks use a radio link instead of cables to connect computers, anyone within the radio range can theoretically listen in or transmit data on the network. Some people feel that the matter of wireless security is a hyped one. In this section, let us discuss how the security issues in wired networks compare vis-à-vis the wireless networks that are relatively new. It is important to examine if wireless networks receive overt attention from security professionals at the cost of ignoring the security of wired networks.

The overall philosophy behind wired networks versus wireless networks is 'trust'. On a wired network, the hardware is under the direct control of the network administrator, and therefore, the overall attitude toward the workstations tends to be one of trust. With a wireless network, it is possible that someone could sit in the parking lot with a laptop and access your wireless network. Therefore, the general attitude toward wireless workstations tends to be one of extreme distrust. However, this difference in attitude often causes the same administrators to take extreme positions when it comes to guarding network security. While they tend to go to extreme lengths at securing a wireless network, at times, they almost neglect wired network security. Things to watch out are the following: are there any unused network jacks or unused switch ports in the office? This is important because if someone was able to sneak into the office and plug a laptop into one of these unused jacks, you may no more have the same level of trust in the hardware on your wired network.

Wireless AP was explained in Box 17.2 in Chapter 17. One of the most basic features included in most wireless APs is a list of workstations that are allowed to access the wireless network. This feature allows entering the *media access control* (MAC) address of each wireless *network interface card* (NIC) owned by an organization. That way, if someone attempts to connect to the network, the AP, it is possible to check if the MAC address of NIC is allowed. If not, then the connection is denied. This technology is not absolutely perfect though. There are still a couple of ways that a hacker could breach the wireless network. For example, some NICs allow you to set the MAC address to an address of your choice. Hackers could spy on the network, get the address of a valid NIC and then assign that address to their own NIC. It is also possible that a hacker could steal one of your NICs and use it to gain access to the network. NIC, as readers are aware, is an expansion board that can be inserted into a computer so that the computer can connect to a network [in the *Further Reading* section, uniform resource locator (URL) links are provided; reader can visit them to know about NIC].

There is another consideration as well. There can be situations wherein a company does not want a wireless network, but employees want it, so they set up their own AP (access point) (see Box 9.2). There have also been cases in which employees are disgruntled because they were not granted access to the wireless AP, so they set up their own AP. These 'rogue APs' can be a serious problem for the corporations. Worse is that setting up a rogue AP is not difficult; an employee does not need a spare network jack to set up a rogue AP. APs usually have a mini-hub built in. Users could just unplug their PC and plug the AP into the network jack that the PC had been using. They can then plug their PC into the AP. Here, MACs come into play; most wireless APs have a MAC address of their own. Therefore, if a wired network has a MAC address filter in place, then the rogue AP would never be able to gain access to the rest of the network.

9.5 Attacks on Wireless Networks

Unauthorized Access to Company Wireless Networks in Organizations

Various types of unauthorized access to company networks are possible in a wireless networking scenario. Figure 9.2 provides a general taxonomy of security attacks to help understand some of the attacks against WLANs, and Table 9.1 provides a brief explanation about each one of them.

We summarize some of the most commonly known security attacks as follows and then discuss each one of them briefly:

1. man-in-the-middle attacks;
2. denial of service (DoS) attacks (briefly mentioned in Table 9.1);
3. network injection;
4. accidental association;
5. malicious association;
6. MAC spoofing for identity (ID) theft;
7. non-traditional networks;
8. ad hoc networks.

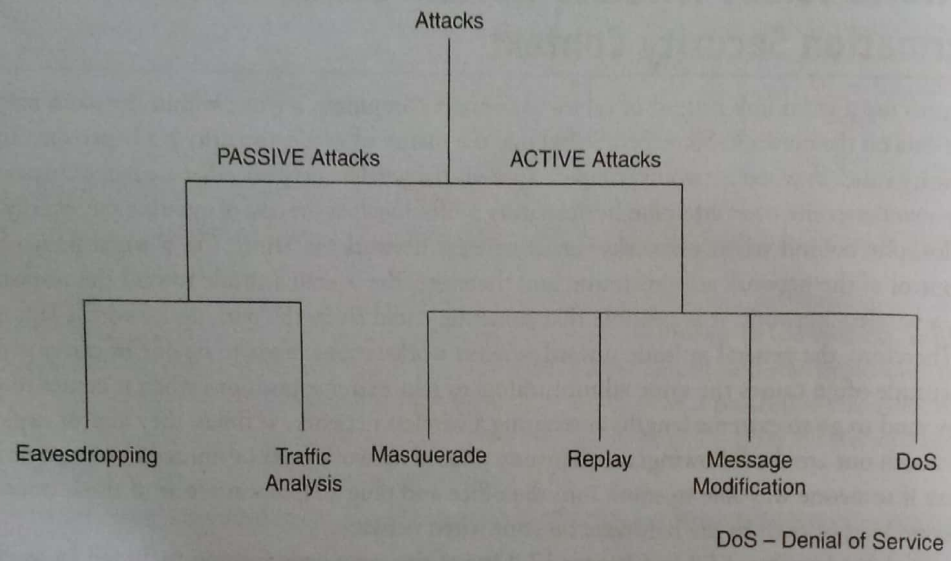


FIGURE 9.2 | Taxonomy of security attacks.

TABLE 9.1 | Security attacks

Type of security attack	What it means
Eavesdropping (compromising confidentiality)	The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
Traffic analysis	The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between the communicating parties.
Masquerading	The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
Replay	The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
Message modification	The attacker alters a legitimate message by deleting, adding to, changing or re-ordering it.
Denial of service (attacking network availability)	The attacker prevents or prohibits the normal use or management of communications facilities.
Jamming (flooding the network with pseudo-packages)	Attackers flood a wireless network with excess radio signals to prevent authorized users from accessing it. Other devices that emit radio signals, such as cordless phones and microwaves, can also disrupt or degrade wireless network performance.

1. **Man-in-the-middle attacks:** We had mentioned this in Chapters 12 and 16. Here we touch upon it in the context of threat to wireless networks. Basically, a 'man-in-the-middle attack' aims at 'sniffing' the network to understand

important information flowing through it. It is one of the more sophisticated attacks planned by crackers. The method revolves around the attacker enticing computers to log into his/her computer that is set up as a soft AP. Once this is done, the cracker connects to a real AP through another wireless card offering a steady flow of traffic through the transparent cracking computer to the real network. The cracker can then 'sniff' the traffic for usernames, passwords, credit card numbers, etc. Refer to Box 9.2; hotspots are particularly vulnerable to any attack since there is little or no security on these networks.

2. **DoS attacks:** Refer to Table 9.1; we have already described this in connection with firewalls and virtual private networks (VPNs; Chapters 16 and 17). A DoS attack occurs when an attacker continually bombards a targeted AP or network with bogus requests, premature successful connection messages, failure messages and/or other commands. These prevent legitimate users to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the extensible authentication protocol, that is, EAP (see Box 9.4).
3. **Network injection:** Recall Box 9.3. A cracker can make use of APs that are exposed to non-filtered network traffic, specifically broadcast network traffic. The cracker injects bogus networking reconfiguration commands that affect routers, switches and intelligent hubs [these components of networking and telecommunication (TC) were discussed in Chapter 13]. Using network injection, a whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

BOX 9.4

Extensible Authentication Protocol

Network protocols were discussed in Chapter 13. The *extensible authentication protocol* (EAP) is a protocol for wireless networks that expands on authentication methods used by the point-to-point protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords and public-key encryption authentication (recall the discussion in Chapter 14 about cryptography and encryption).

EAP is a universal authentication framework frequently used in wireless networks and point-to-point connections. Although the EAP protocol is not limited to WLAN networks and can be used for wired LAN authentication, it is most often used in WLAN networks. To know about the requirements for EAP methods used in WLAN authentication, visit the URL quoted in the *Further Reading* section. EAP sits inside of PPP's authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge–response tokens and public-key infrastructure (PKI) certificates all work smoothly.

With a standardized EAP, interoperability and compatibility of authentication methods become simpler. For example, when you dial a remote access server (RAS) and use EAP as part of your PPP connection, the RAS does not need to know any of the details about your authentication system. Only you and the authentication server have to be coordinated. By supporting EAP authentication, an RAS server gets out of the business of acting as a middle man, and just packages and repackages EAP packets to hand off to a remote authentication dial-in user service (RADIUS) server that will do the actual authentication.

Courtesy:

1. http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol (accessed 11 September 2006).
2. http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol (accessed 11 September 2006).
3. http://www.networkworld.com/details/490.html (accessed 11 September 2006).
4. http://www.networkworld.com/details/490.html (accessed 11 September 2006).

4. **Accidental association:** As we have seen, unauthorized access to a company's wireless and wired networks can come from a number of different methods and intents. One such method is 'accidental association'. This happens when a user turns on his/her computer and it latches on to a wireless AP from a neighboring company's overlapping network. The user may not even know that this has occurred. However, this is a security breach; proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.
5. **Malicious association:** In Box 9.2, we described that establishing a Wi-Fi connection is not difficult. 'Malicious associations' occur when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company AP. These types of laptops are known as 'soft APs' and are created when a cracker runs some

software that makes his/her wireless network card look like a legitimate AP. Once the cracker has gained access, s/he can steal passwords, launch attacks on the wired network or plant Trojans. Recall the open system interconnections (OSI) model introduced in Chapter 13; since wireless networks operate in the layer two (L2) world, layer three protections such as network authentication and VPNs do not offer protection to wireless networks. Wireless 802.1x authentication do help with protection but are still vulnerable to cracking. Crackers exploiting an accidental association may not want to break into a VPN or other security measures. Most likely, they may just try to take over the client at the L2 level.

6. **MAC spoofing for ID theft:** ID theft (or *MAC spoofing*) is a 'passive' threat to the wireless networks. It occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network 'sniffing' capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle. See the *Further Reading* section for some useful website addresses for more information on *ID theft*.
7. **Non-traditional networks:** Non-traditional networks constitute of things such as personal network Bluetooth devices. These networks are not safe from cracking and should be regarded as a security risk. Even bar code scanners, handheld PDAs and wireless printers and copiers should be secured (in Chapter 6, we had considered security issues in the mobile computing scenario). These non-traditional networks can be easily overlooked by IT personnel that have narrowly focused on laptops and APs.
8. **Ad hoc networks:** 'Ad hoc networks' are defined as peer-to-peer networks between wireless computers that do not have an AP in between them. A mobile ad hoc network (MANET) is a kind of wireless ad hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology (see Figure 9.3). The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the larger Internet. While these types of networks usually have a little security, encryption methods can be used to provide security (we have discussed encryption and cryptography in Chapter 14). Ad hoc networks can pose a security threat.

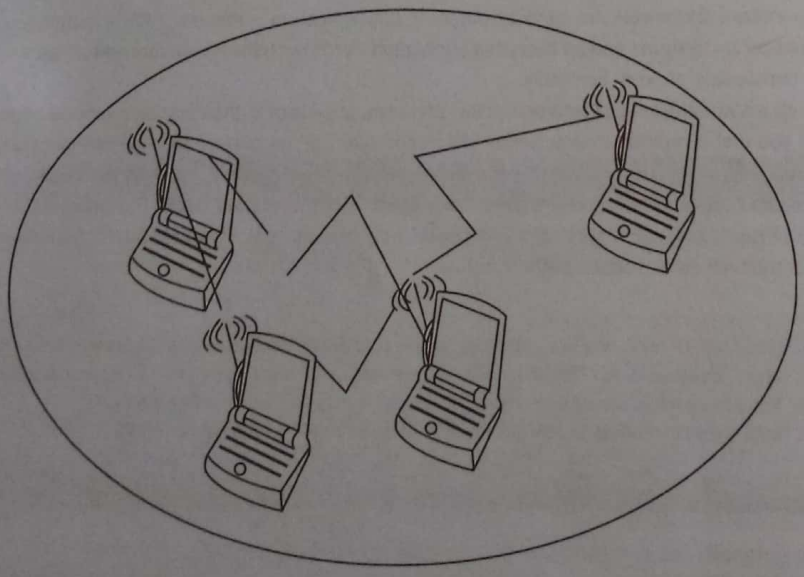


FIGURE 9.3 | Mobile ad hoc network.

Other Security Risks in Wireless Networks

With the prevalence of wireless devices, more users are seeking ways to connect remotely to their own organization's networks. One such method is the use of untrusted, third-party networks. Conference centers, for example, commonly provide wireless networks for users to connect to the Internet and subsequently to their own organizations while at the conference. Airports, hotels and even some coffee franchises are beginning to deploy 802.11-based publicly accessible wireless networks for their customers,

even offering VPN capabilities for added security. These untrusted public networks introduce three primary risks: (1) because they are public, they are accessible by anyone, even malicious users; (2) they serve as a bridge to a user's own network, thus potentially allowing anyone on the public network to attack or gain access to the bridged network and (3) they use high-gain antennas to improve reception and increase coverage area, thus allowing malicious users to eavesdrop more readily on their signals.

By connecting to their own networks via an untrusted network, users may create vulnerabilities for the networks and systems of their organizations, unless their organizations take steps to protect their users and themselves. The users typically need to access information assets and resources that their organizations deem as either public or private. Readers should recall the discussion in Chapter 17 where we covered VPN as a solution to secure connections to the organizations' internal networks. That helps prevent eavesdropping (Table 9.1) and unauthorized access to private resources. Lastly, as with any network, social engineering and dumpster diving (see Box 9.5) also are concerns. An enterprise should consider all aspects of network security when planning to deploy the wireless network.

BOX 9.5

Picking Digital Garbage – *Dumpster Diving* in its New Avatar

This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded. It is also called *dumpstering*, *binning*, *trashing*, *garbing* or *garbage gleaning*. 'Scavenging' is another term to describe these habits. In the United Kingdom, the practice is referred to as 'binning' or 'skipping', and the person doing it, a 'binner' or 'skipper'.

The term originates from the fanciful image of someone leaping into large rubbish bins, the best known of which are produced under the name 'dumpster'. In practice, dumpstering is more like fishing around than diving in. In most cases, people dumpster dive to reclaim items that have been disposed of but can still be put to further use – for example, food, furniture, clothes, etc. In the digital world, 'scavenging' is equivalent of 'dumpster driving'. It is a form in which cast-off articles and information are scavenged in an attempt to obtain advantageous data. Consider, for example, going through someone's trash to recover documentation of his/her critical data [social security number (SSN) in United States, PAN number in India, credit card ID numbers, etc.]. According to a definition in the glossary of terms for the Convoluted Terminology of Information Warfare, 'scavenging' means 'searching through object residue (discarded disks, tapes or paper) to acquire sensitive data without authorization'.

Management Countermeasures and Mitigations for Wireless Network Attacks

In the previous section, we introduced various methods that exist for attacking the wireless networks. In this section, we will discuss some countermeasures and mitigation methods. Readers should make a note that the guidelines described in this section may not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment; at the maximum, they can only help reduce the risk to some extent. It should be clear that there is no 'one size fits all solution' when it comes to security.

Management countermeasures for securing wireless networks begin with a comprehensive security policy. Importance of policy-based controls was emphasized in Chapter 3. A *security policy*, and compliance therewith, is the foundation on which other countermeasures – the operational and the technical – are rationalized and implemented. A WLAN security policy should be able to do the following:

1. Identify who may use WLAN technology in the organization (employees, suppliers, customers, business partners and other similar affinity organizations; recall the concepts of 'extended enterprise' introduced in Chapter 1).
2. Identify whether Internet access is required for 'everybody' in the organization and consider providing access on a 'need-to-know' basis.
3. Describe who can install APs and other wireless equipment for use in the organization.
4. Provide limitations on the location of and physical security for APs.
5. Describe the type of information that may be sent over wireless links.
6. Describe conditions under which wireless devices are allowed (in Chapter 6, we had introduced the security risks arising out of usage of mobile handheld devices by those connected with a business enterprise).
7. Define standard security settings for APs taking help from network technical experts.
8. Describe limitations on how the wireless device may be used, such as location.

9. Describe the hardware and software configurations of all wireless devices.
10. Provide guidelines on reporting losses of wireless devices and security incidents.
11. Provide guidelines for the protection of wireless clients to minimize/reduce theft.
12. Provide guidelines on the use of encryption and key management.
13. Define the frequency and scope of security assessments to include access point (AP) discovery.

Mitigation means to reduce the probability of an adverse event or its impact in the course that the adverse event realizes. We will discuss some well-known techniques as follows:

1. **Using encryption:** Cryptography and encryption were discussed in Chapter 14. Today, most organizations use 'encryption' as a mandatory practice. Would you communicate across a wireless network without using encryption? Of course not, but many of the wired networks allow the majority of communications to go unencrypted. Wired networks are just as prone to eavesdropping as wireless networks are. The only difference is that wireless networks can be 'snooped' on by outsiders, and snooping on a wired network requires a physical connection. Even so, there are plenty of instances in which an employee with malicious intentions may use a protocol analyzer to spy on coworkers. However, many companies choose to only encrypt traffic flowing between servers. Although there are certainly exceptions, the bulk of the traffic flowing between servers and workstations is typically not encrypted. We must understand, however, that none of the network solutions are without implications. For example, a couple of years ago, conventional wisdom stated that most workstation traffic should not be encrypted because of the burden that encryption places on the network. The encryption and decryption process consumes processing power, and encrypted packets typically consume more network bandwidth. Although these may have been valid arguments at one time, it is now time to encrypt all network traffic. Network cards exist that can handle the encryption and decryption process without having to burden the processor. Likewise, *gigabit network cards* (these are basically network adapter cards for increasing the access speeds; see the URL quoted in the *Further Reading* section) have become cheap enough so that the extra bandwidth required by the encrypted packets should no longer be a huge issue.
2. **Network isolation:** One of the other ways that wireless network security has surpassed wired security is in the way that it is isolated. In many companies, anything coming in through a wireless AP is automatically assumed to be non-trustworthy, until the sender can prove otherwise. Because the air waves are assumed to be an insecure medium, wireless traffic is handled in a different way than wired traffic. Companies will typically establish a VPN for wireless users (VPNs were discussed in Chapter 17). The idea is that when users attach to a wireless network, they are completely isolated from the rest of the network until they have been authenticated. Often, the authentication mechanism is not even allowed a direct access to a domain controller. Instead, a remote authentication dial-in user service (RADIUS) server is typically used to authenticate wireless users. Once authentication has been established, the user communicates with the network through a secure tunnel. Readers can refer the quoted website in the *Further Reading* section to learn more about 'RADIUS authentication'. VPNs use their own encryption. At the same time though, the wireless signal is already encrypted. This means that legitimate wireless traffic is double encrypted, using two completely different encryption protocols. In summary, we note that wireless security mechanisms need to be far more stringent than those used on wired networks.
3. **Restricting wireless access and filtering out intruders:** If an AP allows it, corporations should restrict wireless access to office hours or whenever the network is expected to be under use. However, given the modern times and the dominance of IT workers who do not restrict themselves to regular 9–6 h, this is not easy. As discussed previously, each network card has a unique code called a MAC address. APs can be set to restrict network access to trusted MAC addresses. Though this technique is not foolproof, it is said to help.

Physical security was discussed in Part II of this book; its relevance can be explained in the context of protection of wireless networks. In maintaining InfoSec, physical control of wireless-enabled devices takes on more importance. Areas of physical risk include the placement and configuration of wireless APs and control of the wireless-enabled device that connects to the organization's network. For example, it can be difficult to control the distance of wireless network transmissions, because wireless APs can broadcast signals from 150 ft to as far as 1,500 ft, depending on how they are configured. As a result, wireless APs can and do broadcast signals outside building perimeters.

Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity and lower installation costs. However, risks are inherent in any wireless technology. To many, the term 'wireless network' has become almost synonymous with the term 'insecure'. Ever since wireless networks first started becoming popular, the Internet has been replete with stories of wireless security nightmares. Wireless networks face all of the InfoSec risks that are associated with conventional wired networks, such as worms and viruses, malicious attacks and software vulnerabilities, but there are significant challenges that are unique to the wireless network environment. Organizational security policies play a major role when it comes to protecting wireless networks. When installing wireless networks, it is crucial for the organizations to implement controls – such as developing wireless security policies, configuring their security tools to meet policy requirements, monitoring their wireless networks and training their staffs in wireless security. Countermeasures and mitigations in view of threats to wireless networks include both operational and technical aspects. VPNs, firewalls, intrusion detection systems (IDSs) and encryption are important aspects in wireless network security. The key point in this chapter is that protecting a wireless network requires forethought and planning, just as protecting a wired network does.

Review Questions

1. Explain the term 'Wi-Fi'. What are 'ad hoc networks'?
2. Explain how the Bluetooth technology is supporting wireless communications.
3. Discuss if security considerations in the wireless world should be different than those in the wired world, providing supporting arguments based on your observations and experiences with the technology.
4. Who are 'crackers' and what are their motives? How do they work?
5. What roles do the media access control (MAC) and access points (APs) play in wireless security?
6. What different methods have you learned in this chapter that are used for launching attacks on wireless networks?
7. In the light of the discussion in this chapter, explain what is at stake and how if the wireless networks are not protected.
8. How do you distinguish 'active attacks' from 'passive attacks'?

Further Reading

Arbaugh, W.A., Shankar, N. and Justin Wan, Y.C. (2001), *Your 802.11 Wireless Network has No Clothes*, Paper presented at Department of Computer Science, University of MD, USA.

Brenton, C. and Hunt, C. (October 2002), *Mastering Network Security*, Sybex, San Francisco, CA, USA.

Dean Vines, R. (July 2002), *Wireless Security Essentials: Defending Mobile Systems from Data Piracy*, John Wiley & Sons, IN, USA.

Gehrmann, C., Persson, J. and Smeets, B. (June 2004), *Bluetooth Security*, Artech House Computer Security Series, MA, USA.

Godbole, N. (2005) *Relating Mobile Computing to Mobile Commerce, Handbook of Research on Mobile Business: Technological, Methodological and Social Perspectives*, Reference Book, Idea Group, Inc., Hershey, PA, USA (ISBN: 1–59 140-817-2, Chapter XXXIII).

http://longwood.cs.ucf.edu/~turgut/COURSES/EEL5937_MANET_Spr03/EEL5937_Schedule_Spr03.html (accessed 10 September 2006) to understand about *Mobile Ad-hoc Network* (MANET) (this site contains pointers to research work and other knowledge assets in the domain http://www.olsr.org/docs/report_html/node9.html)

http://support.3com.com/infodeli/inotes/techtran/4bba_5ea.htm (accessed 17 March 2008) to read about PCMCIA cards.

http://tools.ietf.org/html/rfc4017, http://www.faqs.org/rfcs/rfc2284.html, http://www.ietf.org/rfc/rfc2284.txt and http://www.networksorcery.com/enp/protocol/eap.htm (accessed 11 September 2006) to understand the requirements for the EAP Protocol (*Extensible Authentication Protocol*).

http://www.bellaonline.com/articles/art35075.asp and http://bugclub.org/beginners/networking/NetworkCard.html (accessed 12 September 2006) for useful information about *Network Interface Card*.

http://www.cheapcomputersale.com/gigabit-net work-cards.php (accessed 12 September 2006) for *Gigabit Network Card* information.

http://www.es.net/raf/ESnet-RAF-WP.doc (accessed 13 September 2006) to understand about *RADIUS Authentication*.

http://www.identitytheftprotection.org.uk/, http://www.usdoj.gov/criminal/fraud/idtheft.html, http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm and http://www.idtheftcenter.org/index.shtml (accessed 9 September 2006) for good information, articles, etc., on *Identity Theft*. http://www.wardrive.net/security/links (accessed 13 September 2006) for links to *Wi-Fi Security* articles and papers.

The Internet of Things (IoT) and Smart Cities: Security and Privacy Challenges

10

Learning Objectives

After completing this chapter, you will be able to:

- understand what the *Internet of Things* (IoT) is and how it has emerged.
- appreciate the concept underlying the *IoT*.
- learn the benefits of IoT and how it impacts our life.
- get a brief overview of how IoT works.
- understand the concept of 'Smart Planet'.
- learn about the Security and Privacy challenges in the IoT.
- understand the role of IoT in *Smart Cities* and *Intelligent Buildings* in the high-tech world.
- develop an understanding of Security and Privacy challenges with IoT, Smart Cities and Intelligent Buildings.

10.1 Introduction

The concept of the 'Internet of Things' (IoT)is very interesting indeed. In the domain of electronic commerce, we hear the terms B2B (*Business to Business*), B2C (*Business to Consumer*) wherein businesses talk to businesses and businesses talk to their customers. 'Talking' in this context means communicating mainly through the business portals developed. Now comes the era in which 'things' talk to 'things'. To some people this may sound like a scary proposition, while to others it may be a very exciting one! In this chapter, we want to understand the security and privacy challenges in IoT and the spheres of life and businesses touched by IoT – this includes smart cities too. To appreciate such new scenarios, we first need to understand *what* and *how* of the 'IoT'– how it has emerged and how it works. We shall also present the overarching implications of IoT; especially in the context of 'smart' cities that also include 'intelligent buildings'. The chapter ends with the discussion about security and privacy implications of these paradigms. Thus, in a larger part of this chapter, IoT and its related aspects are explained and then the emerging security and privacy issues are discussed. In the reference section, several information sources are listed which serve as an extended study material for those who wish to explore further on the topic. The review questions at the end help you to assimilate what have you learned in the chapter.

10.2 The 'Internet of Things' (IoT): The New Kid on the Block

The Internet is considered to be one of the most or the most fantastic revolution or invention of our times; it has gone through evolutionary phases, and yet it is said to be a relatively 'young' technology:

- 1969–1995: Early years of Internet development and its spread.
- 1995–2000: Internet of the 'geeks' (techno-freaks or gizmo-loving techies).

- 2000–2007: Internet of the 'masses' (wide spread of commoners' use of the Internet).
- 2007–2011: Mobile Internet.
- 2012 and beyond: Internet of the Things (IoT).

The IoT has become a hot topic of conversation and sometimes also a topic of controversy. The IoT concept not only has the potential to impact our way of living but also the way we work. It is good to understand what exactly the IoT is and its impact on our life and workplaces, if any. While there are technological complexities involved, IoT let us appreciate the basics to grasp the foundation. Kevin Ashton was the first one to coin the term *Internet of Things* (IoT) in 1999. It refers to uniquely identifiable objects (things) and their *virtual representations* in an Internet-like structure. Figure 10.1 shows a schematic representation of such arrangement. Almost every year, there are engineering innovations to integrate more and more digital devices with the Internet!

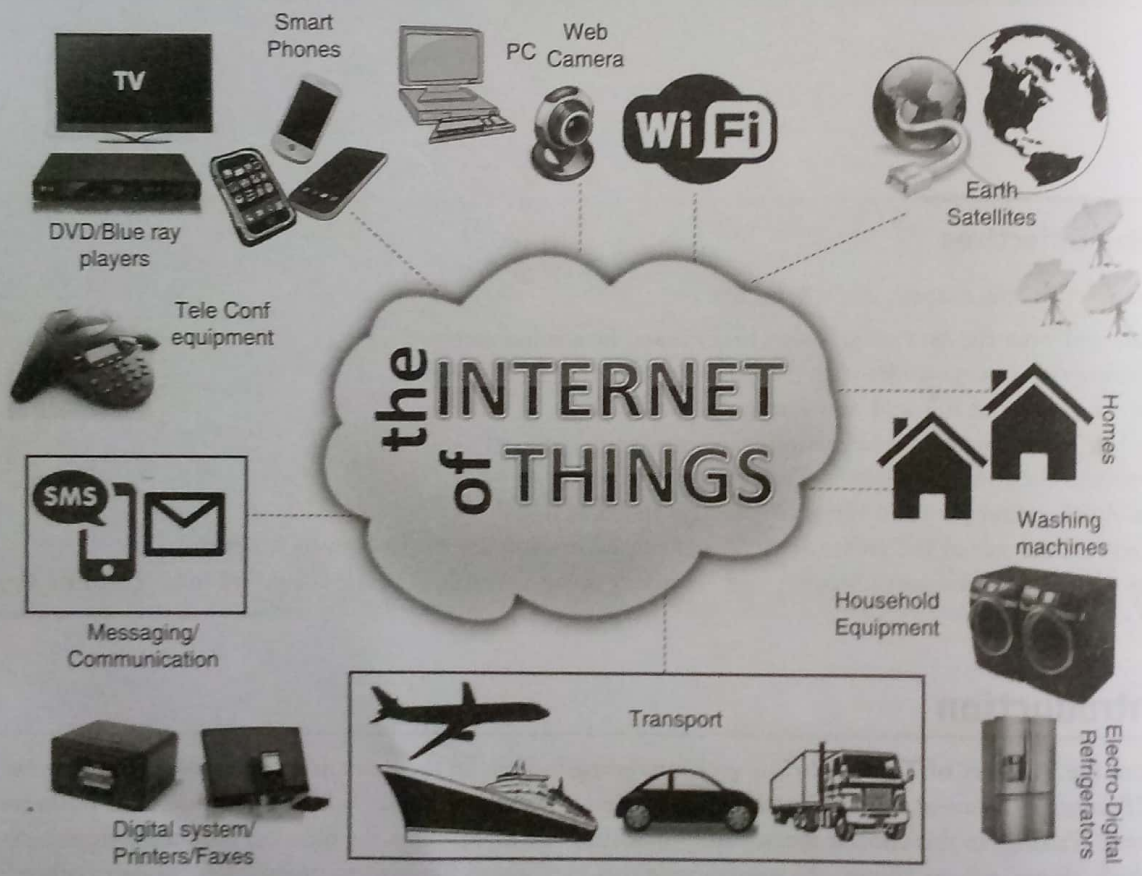


FIGURE 10.1 | The Internet of Things (IoT): The concept.

We know that computers have 'Internet protocol' (IP) address'; in the world of IoT, there are digital devices (capable of 'communicating') that have IP addresses (the concept of 'IP address' is explained in Chapter 13 – refer to Figure 13.7). The IoT concept further extends the anytime-anywhere idea of communication to make it 'anything-anytime-anywhere' communication. With IoT (i.e., 'talking' objects), almost everything in daily life will be identifiable, addressable and traceable. This is because, as mentioned, all the things in the IoT networks are interconnected with either wired or wireless networks (i.e., through digital methods of communication). In such a paradigm or literally in such a scheme of 'things', any device that can be hooked up to the Internet can be controlled through the Internet and can also be accessed through the web; often they are smartphone or similar devices. In this context, you may like to revisit or read Chapter 8. In reality, 'Things' are simply the ploys for collecting data, listening devices and information recorders. According to some people, IoT is nothing but a marketing scheme or a ploy to get more of your 'data'– remember the concept of Big Data in Chapter 7. In the 'smart' digital world, everyone is after your data, more data and more data and so on, in the name of business analytics and many other similar fancy terminologies, sometimes for a real good cause, sometimes for causes that may not be so good, and herein lies the security and privacy threats from the world of IoT.

IoT does have implications for '**SmartCities**' and '**Intelligent Buildings**' as we shall see in the later sections of this chapter – Sections 10.4.1 and 10.5.

It will help you to revise the concepts mentioned in the previous sections, by referring to the other chapters mentioned below.

The concept of **IP address**: refer to Figure 13.7 in Chapter 13.

Smart Phone Security: refer to Chapter 8.

IoT: The Context

Refer to Figures 10.1 and 10.6; to put it simply, the *IoT* is an emergent network of *everyday objects* – these objects range from the very simple ones to some that are very complex, that is, from industrial machines to goods that consumers use. What makes it interesting is that these 'objects' have got an embedded technology inside them that makes them capable of sharing information as well as completing tasks while the users of those objects are busy with other activities (e.g., when users work, sleep or exercise). To get an idea as to what this could mean, refer to the discussion about *intelligent software agents* (Section 28.7.6, Chapter 28); the scenario presented in Box 28.17 gives us an idea about the concept of IoT although the objects (i.e., 'Things') networked through IoT may not always be or work like what the 'intelligent software agents' do. One thing for sure, the idea behind IoT is to build 'intelligence' in the devices that we use, so as to make them 'smart'.

It will also help you to read the scenario presented in Box 28.17, Chapter 28.

With the advent of IoT, the day is not far when most of our major appliances (smart phones, refrigerators, washing machines, VCD players or equivalent devices, etc.), our cars (in their new avatar called 'smart cars'), our homes (inside 'intelligent buildings' see Figure 10.11), and even our city streets will be communicating through the Internet (see Figures 10.1 and 10.2). When this happens, the result is the creation of 'network of objects' and such a network is called the 'IoT'. The IoT, which is composed of millions of sensors and devices that generate continuous streams of data, can be put at the service of us humans to improve our lives and our businesses in many ways that we could not have imagined. The question is how does it all work? Will it work so seamlessly? And what are these 'things' that are 'woven' as the part of the network? Let us understand all this.

BOX 10.1

Sensors and Actuators

There are sensors that generate an expected format of data and non-personal information. Some physical sensors are Thermal Sensors, Light Sensors, Presence Sensors, Magnetic Sensors, Radio Frequency Identification (RFID) tags.

A sensor is used for gathering information from the environment. An actuator represents the methods in which the information gathered by the sensor is processed or not, and is sent back to the user. Suppose there is a system designed for collecting information about traffic and suppose this system works as a combination of twitter with physical traffic sensors. Suppose this system is designed to send back the information about the traffic scenario in different parts of the city to a certain traffic-related 'App' (i.e., software application) on driver's Smartphone. In this case both the Application (installed on the Smartphone) and the Smartphone are example of actuators.

Actuators can be one of two types – Direct or Indirect; such a classification depends on the access to the information. For example, the access can be: (1) direct, like on a Smartphone or (2) indirect, like through a smart panel.

Broadly speaking, IoT is an information network that connects physical and virtual objects. There are three main components in an IoT:

1. The things (or devices or assets) themselves.
2. The communication networks that connects them (to make them communicate with each other).
3. The computing systems for using the data that flows to and from those 'Things'.

Once those objects/assets/devices are woven inside the communication infrastructure, they can communicate with each other and even optimize activities between them using the analysis of data that flows through the network. In the IoT world, each of the 'thing' that communicates with the other over the Internet, has to have its IP address (the concept of IP address is explained in Chapter 13). IoT is the future (some of it is already happening) wherein all sorts of digital devices and sensors communicate with one another as well as with distant computers and other systems to operate in a seamless fashion to transform our world. For the communication to take place, we need some sort of network. While some devices might be hardwired into an existing network, others will need to communicate wirelessly and securely (see Chapter 9). Ideally this should be implemented through *mesh networks* (network topologies are explained in Section 13.4 of Chapter 13). In networks based on 'mesh' topology, nodes relay information across the network. Various devices and sensors could operate as those nodes. Mesh topology enables a robust communication across the network because even if one node fails, other nodes can route the information to where it needs to go (see Figure 10.2).

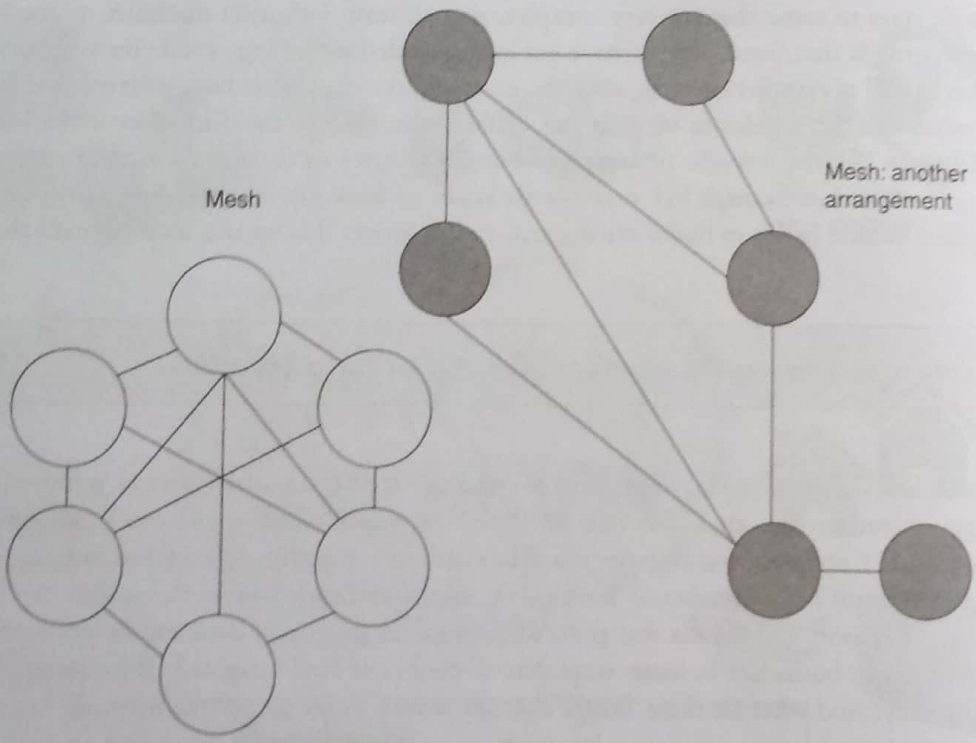


FIGURE 10.2 | Mesh topology.

Security of Wireless Networks – see Chapter 9.
Network Topologies (mesh networks, etc.) – see Section 13.4 of Chapter 13.

For 'Privacy' fundamentals, visit Chapter 27.

The general thinking in understanding catchwords such as IoT is that a there exists a group of inanimate objects that are enabled with wireless connectivity integrated inside those objects, with the objective that those objects can be monitored, controlled and linked over the Internet via a mobile application.

The categories of objects can be of a wide variety, ranging from light bulbs that one can 'wear' to appliances used in homes (e.g., washing machines, coffee makers, cars) – almost anything into which **Wi-Fi connectivity** can be designed.

These days, IoT is also being applied to **medical and healthcare industry** that has many vertical markets. IoT is being applied to transportation systems where RFIDs play a significant role.

Arguing that **devices contain 'data'** (personal data of a user including his/her movement tracking or business data of an organization including 'movement' of products), the very concept is antecedent of '**privacy' violation**!

RFID technology, active and ***passive RFID tags***, etc.– see Chapter 28.

How Does the IoT Work?

Let us first understand how IoT works, without getting technical. Simply put, IoT devices have a radio that they use to send and receive wireless signals. There are IoT wireless protocols designed to establish some basic communication services. Such protocols operate on low power, they consume low bandwidth and they work on an implementation of mesh network (see Figure 10.2). Some IoT devices operate on the 2.4 GHz band, which is also used by Wi-Fi and Bluetooth, and the sub-GHz range. The sub-GHz frequencies, including 868 and 915 MHz bands, may have the advantage of less interference. Thus, first and most important is the underlying technology – the Internet as well as the numerous wireless radios that allow these devices to connect to the Internet and most importantly, to each other. A number of communication standards are involved (see Box 10.2 – IoT Communication Standards Biz-E-Bee, ZigBee and Others), for example, the familiar ones like Wi-Fi, low-energy Bluetooth, Near Field Communication (NFC) and RFID. There are also others that we do not frequently hear of, for example, ZigBee, Z-Wave and 6LoWPAN. Apart from these standards, there are the things themselves – 'things' or objects such as motion sensors, door locks, light bulbs, etc. (see Figures 10.1 and 10.5). In some situations, there may also be a central 'hub' that allows different devices to connect to one another.

BOX 10.2

IoT Communication Standards: Biz-E-Bee, ZigBee and Others

ZigBee

ZigBee is a mesh network (refer to Figure 10.2) specifications for low-power wireless local area networks, that is, WLANs that cover a large area. The standard was designed to provide high data throughout in applications where the duty cycle is low and low power consumption is an important consideration – and this is very much true for 'intelligent buildings', they are supposed to be energy efficient. ZigBee uses a specification for a suite of high-level communication protocols used to create personal area networks built from small, low-power digital radios based on an **IEEE 802.15.4** standard.

NFC

Near field communication (NFC) smartphones and other devices use the set of protocols to establish radio communication with each other – this can be done by touching the devices together or bringing them into proximity to a distance of typically 10 cm (3.9 in.) or less.

Z-Wave

Basically, Z-Wave is a radio frequency control protocol designed to achieve dependable communication and operation between diverse products provided by different manufacturers. Z-Wave can be used on your tablet or smartphone to control your environment when you are at home. It is used for home automation.

6LoWPAN

6LoWPAN is an acronym to combine into a single word, the terminology that is based on the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, empowers the smallest devices with limited processing ability to transmit information wirelessly using an IP. ZigBee is the latest competitor to 6LoWPAN.

As broadband Internet becomes more widely available, the connection cost decreases; as a result, more devices are being created with Wi-Fi capabilities and sensors built into them. Technology costs are also going down, and smartphone penetration rate is high like never before. All of these factors are driving a 'storm' for the IoT. We know that day-to-day devices can have an 'on–off switch' – the idea of connecting any device with an on and off switch to the Internet (and/or to each other) embraces everything from communication devices such as tablets, cell phones, home appliances (e.g., lamps, wearable devices, coffee makers, washing machines, headphones) and almost anything else we can think of. The concept also applies to machine components, for example, a jet engine of an airplane or the drill of an oil rig. If the device has an on and off switch then, most probably, it can be a part of the IoT. Gartner Predictions (the research analyst firm) estimate that by the year 2020, there will be over 26 billion connected devices. This is a mind-boggling number of connections! According to other predictions, the number of 'connected devices' may even be much higher than that (i.e., over 100 billion). This giant named 'the IoT' is a massive network of connected 'things' (which also includes people) giving rise to the relationship between people–people, people–things and things–things. Figure 10.3 shows some examples of wearable (digital) devices. More examples of wearable devices are shown in Figure 10.4.

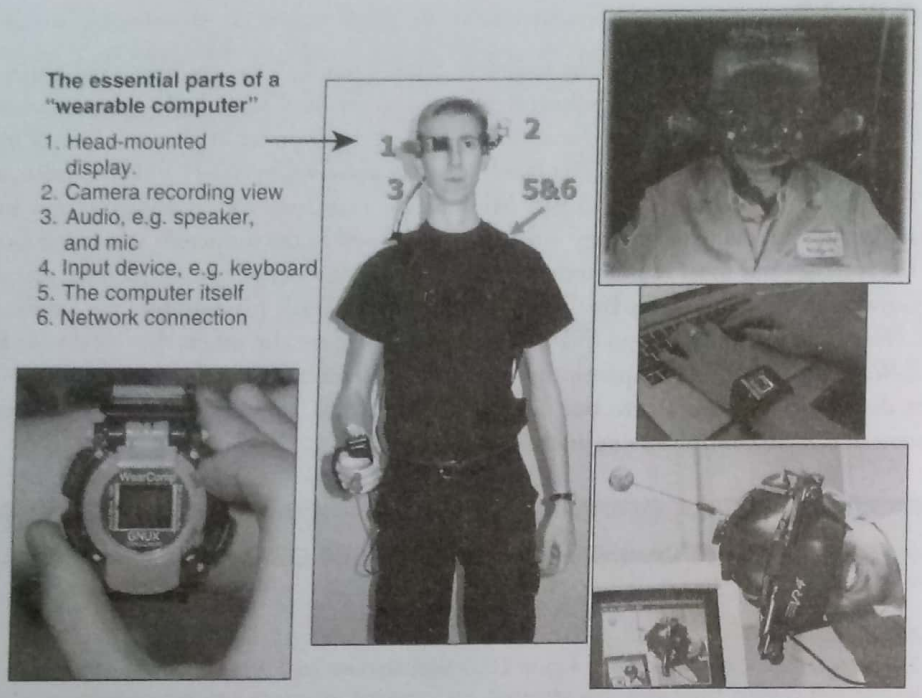


FIGURE 10.3 | Examples of wearable devices.

FIGURE 10.4 | More examples of wearable devices.

From a technical perspective, it is best to look upon IoT as a system of blocks of houses that we have in any typical city except that 'buildings' are not really buildings but rather entities for digital communication – refer to Figure 10.4; it shows the architecture of the Internet which is the foundation of IoT. Therefore, to understand how the IoT works, we need to understand how the *Internet* works. It is convenient to look at it,that is, the Internet as an analogy to a system through which the postman delivers letters to houses in each area. It would be useful to visit Figure 13.7 in Chapter 13 wherein the concept of 'IP address' is explained.

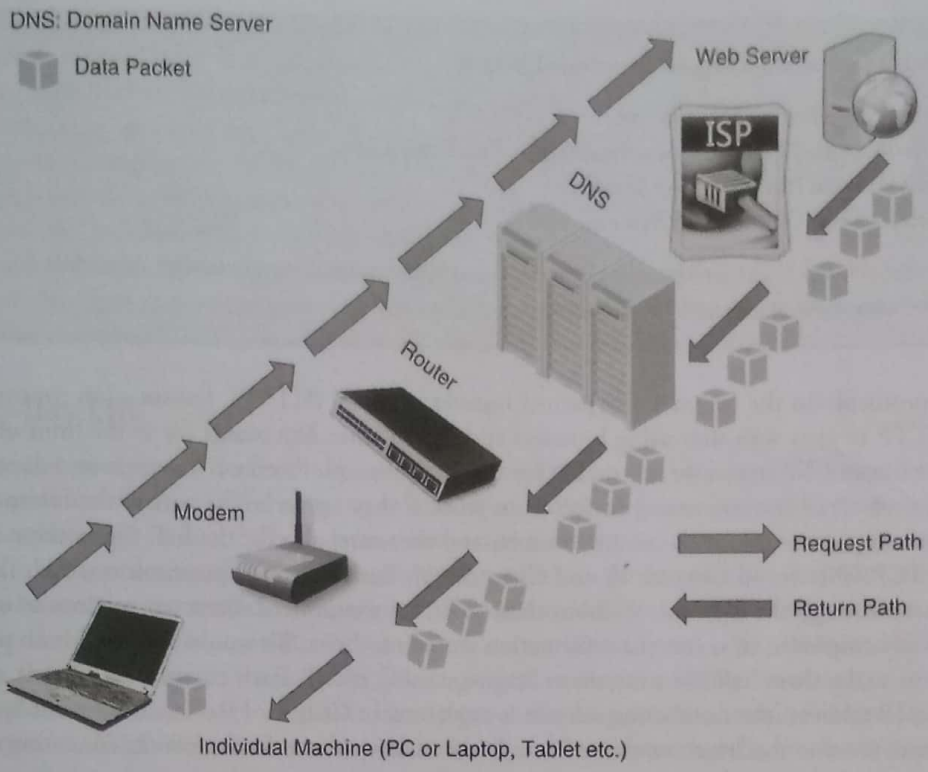


FIGURE 10.5 | The architecture of Internet.

To understand how the IoT work, we need to understand its underlying infrastructure, that is, **how the Internet system works**.
You need familiarity with the **network protocols** mentioned in this section onward.

The Internet is a system with two main components: (1) the **Hardware elements** and (2) the **Protocols**. The first of those components – the hardware component – includes everything from the cables that carry terabits of information every second to the computer sitting in front of you. Cell phone towers, routers, servers, smartphones, satellites, radios and other similar types of devices are the hardware components supporting the Internet. The network, that is, network of networks is formed of all these devices put together. The Internet is a flexible system; in that, it changes in little ways as new elements join and some elements may leave networks around the world. However, some of those network elements may stay on to form the mainstay of the Internet. Others are more of peripheral devices. These elements in the network form connections; it is a 'connected world'. The connected world consists of a number of elements: (1) end points or clients, (2) servers, (3) nodes and (4) data transmission lines. Some of the elements (e.g., the computer, smartphone, etc.) that we use to read the stuff on the Internet of information, are the *end points* – they may count as one. Those end points are denoted as *clients* whereas *servers* are the machines that store the information we search on the Internet. In addition to this, there are other elements called *nodes* which serve as a connecting point along a route of (data) *traffic*. Then there are the *transmission lines* – they can be physical, as in the case of cables and fiber optics, or they can be wireless signals from radios, cell phone satellites, 4G towers, etc.

The second component of the Internet is very important because without this component the hardware elements mentioned in the first component would not create a network. The second component of the Internet is the *protocols*. Protocols are simply the sets of rules that computers follow to complete tasks assigned to them. Communication between devices connected on the Internet could not happen unless there is a common set of protocols that all components (including computers) connected to the Internet must follow. The plethora of machines on the Internet, that is, the computers would not understand one another or even send information in a meaningful way if these protocols did not exist. The protocols, thus, provide both the method and a common language for machines/computers to use the data received and also to transmit data. Let us understand the protocols and how information that gets transmitted across the Internet.

You may like to revisit or read the chapters mentioned below:

Chapter 12: Network Security in Perspective.
Chapter 13: Networking and Digital Communication Fundamentals.
Chapter 17: Virtual Private Networks for Security.
Chapter 18: Security of Electronic Mail Systems.

You can also visit the related **links in the reference section;** those links contain **useful materials** for understanding greater details of the **concepts explained in this section**.

There are several protocols on the Internet – hypertext transfer protocol (HTTP), transmission control protocol (TCP) or IP. We use the HTTP to view web sites using browsers and that is what *http* stands for at the front of any web address that we see. When we use an FTP server, we rely on the file transfer protocol. Protocols like these and dozens of others form the framework within which all the connected devices must work if they are to be the part of the Internet. TCP and IP – these two are the most important protocols on the Internet, and therefore, also for the IoT. Often these two protocols are grouped together as TCP/IP (refer to Chapter 12 and Chapter 13). Basically, these protocols establish the rules to decide how information passes through the Internet. Without these rules, we would need direct connections to other components of the network, such as computers, to access the information stored on them. We would also need both our computer and the target computer to make them 'talk' in a common language using the IP. Each component, that is, device connected to the Internet has an IP address (the numbering scheme is explained in Chapter 13). This is how one machine/computer can 'find', that is, detect another machine/computer through the massive network of networks consisting of thousands and thousands of them.

The most commonly used version of IP currently (at the time of writing this book) is IPv4. It is based on a 32-bit address system. However, there is one problem with this system: given the massive number of machines in the network, we are falling short of addresses. That is why long back in 1991, the Internet Engineering Task Force figured out that it was necessary to develop a new version of IP to create adequate addresses in order to meet growing demand. As a result of this, IPv6, a 128-bit address system was developed. It is believed that it supports the number of addresses to accommodate the rising demand for Internet access for the imaginable future. When we want to send a message or retrieve information from another machine/computer on the network, the TCP/IP protocols are what make the transmission possible. Our request to search information hits the domain name servers (DNS) when it goes out over the network of networks, that is, the Internet and along the way it finds the target server. The DNS sends the request in the right direction. Once the server at the target destination receives the request, it can send a response back to our requesting computer. However, while coming back to us, the data might travel a completely different path (see Figure 10.4). The Internet is such a powerful tool because of this flexible approach to data transfer. Now, let us understand in greater details how information travels across the Internet (basically about the *data packets* mentioned in Figure 10.4). Data packets are those that constitute the 'information' traveling on the network.

In a typical session for using the Internet, we first open the web browser to be able to connect to our website. When we do this, our computer sends an electronic request over our Internet connection to our Internet service provider (ISP). The ISP then directs the request to a server further up the chain (a chain of computers) on the Internet. Finally, the request reaches a DNS (refer to Chapter 12 to understand the concept). Now, this server looks for a match for the domain name we have typed in (e.g., www.google.com). If a match is found, it will direct our request to the IP address of the destination server. If there is no match, it will send the request further up the chain to a server that would (hopefully) provide more information. Finally, the request will come back to our web server (from where we started). Our server will reply by sending the requested file in a series of (data) packets. Packets are parts of a file that vary between 1000 and 1500 bytes. Packets have headers and footers that tell computers what a data packet contains and how the information fits with other packets to create an entire file. Each packet travels back to the network and then to your computer (see Figure 10.4). All (data) packets do not necessarily take the same path; they generally travel the shortest possible path (because that is how the algorithms are designed). Note this important feature – data packets can take up several paths to reach their final destination and it is possible for information, that is, data packets to go around busy areas on the Internet. Actually, as long as some connections are available, information, that is, data packets could still travel from one segment of the Internet to another; nevertheless, it might take longer than it would have taken in normal circumstances.

When the data packets reach us, our device, that is, the computer or equivalent device (say smartphone or tablet) arranges them according to the protocol rules. Imagine this like a jigsaw puzzle being put together according to the preset rules. Finally, we see the information requested on our computer (say an article, a move, a news items, etc.).

The process or sequence of events mentioned is applicable to other kinds of files as well. For example, when we send an electronic mail, it gets decomposed into data packets before it gets sent across the Internet. Internet phone calls, too, convert conversations (which is nothing but bits and bytes of data) into (data) packets using the voice over Internet protocol. Network pioneers like Vinton Cerf and Robert Kahn have done all great work for these protocols – for us to enjoy all this at the blink of an eyelid! In short, this is how the Internet works while the processes taking place in the background are quite complex. Now that we understand that the IoT uses the basic Internet infrastructure and how the communication over the Internet works, let us turn to devices that work for us connected through the IoT.

IoT in Day-to-Day Life

Nowadays, we see the word 'smart' prefixed often to many everyday objects – for example, *smart locks*, *smart thermostats*, *smart cars*, *smart cards* and what not. We are going to hear these terminologies more in the year to come on. Hence, a key question is what makes them so smart? These devices connected through the Internet, are all part of the IoT. As explained earlier, IoT refers to the connection of everyday usage objects not only to the Internet but also to one another – with the goal to provide users with smarter, 'more efficient experiences'. Let us consider one example of this – due to rising security issues, homes (in developed countries) are getting more automated, as new 'smart home' products most of them are controlled by smartphone apps, that is, applications are available. One such lock is called the August Smart Lock – a small video clip about this 'smart lock' (August wireless door lock that is battery powered and connects through Bluetooth) can be viewed at the URL (http://recode.net/2014/10/14/review-a-high-tech-door-lock-thats-also-simple/). From physical security perspective thought and according to the author's viewpoint and experiences, it would be only slightly inappropriate even if, in the world of IoT, one could turn on the lights, start the coffee maker and adjust the thermostat just by sneezing at the right time and place, that is, to say at a flick of a button on your smartphone to throw the IoT connected devices to work. It is said that the trouble with many of these IoT-based products is that they can be complicated, prone to software errors, network issues. Sometimes they also happen to be part of often-incompatible networks that try and do so much (correctly) that they make your head spin or may just stop working to give you a heartache; in either case, your best bet is to go visit your most trusted physician!

Let us consider some day-to-day scenarios wherein IoT plays a role in our life; in some developed countries, this is already happening. The first scenario concerns working mothers (typically in countries like India, while in foreign countries, the same worry may haunt working young fathers) whose greatest anxiety is to be able to monitor their babies (left at crèches or with babysitters) while they work. Now through their smartphones, working parents will be able to monitor their baby's activities and overall well-being. Babies will wear IoT connected devices that will transmit an alert to their young parents when there is anything abnormal with their health, for example, body temperature, convulsing, vomiting, etc. Thus, they can see how well their children's potty training is working – no more a dream or an imagination. This is how young parents will reap the benefits of IoT connectivity. On similar lines, IoT connected devices make possible pet monitoring systems to allow pet keepers to monitor their activity and behavior even when they are away from them. They can also monitor, for example, how honest their dog walker really is.

Another scenario of IoT benefits comes from health arena. Suppose your medicine prescription is running low; your IoT connected device will make an appointment with your physician through your contact list in your smartphone. Doctors will be able to monitor how often and when their patients are taking their medicine; as their IoT connected devices (i.e., a doctor's device connected with that of his patient) shall send notifications regarding this. People with repeated health issues will be able to get their blood pressure and sugar levels monitored remotely even when on the move as such monitoring devices will be connected through IoT technology.

See Box 10.3 and also refer to Figures 10.1 and 10.5. One of the ideas behind the emerging concept of 'smarter planet' is to be 'green', that is, energy efficient as global warming is the biggest concern for all of us. IoT is going to be a solution in this area as well. Household appliances will be connected through IoT and their energy consumption will not only be monitored but also be adjusted based on electricity consumption tariff to lower people's electric bill. Thermostats and lighting will learn our habits and using that electricity consumption data, they will create the optimal setting based on our daily life, for example, turning to our ideal temperature just before one arrives home. These gadgets will also have the capability to sense when no one is in the house and turn off automatically to reduce wastes and costs;

as we know light sensors and movement sensors already exist; now IoT would allow us to integrate their signals with our daily use devices.

Another scenario of IoT in day-to-day life revolves around traffic jams. Driving is a painful experience in most large cities. It is predicted that with IoT devices, driving is likely to become safer (if not easier!). Real-time traffic conditions data fed into traffic lights will help them get adjusted to peculiar conditions such as when an ambulance, a fire-brigade team or other emergency vehicle is approaching. Road sensors will be able to adjust to the speed limit based on data about accidents and weather fed to them; at the same time, they will be communicating directly to car dashboards about unsafe conditions (e.g., slow down, work in progress in some segments of the roads or any other hazards on the way, tricky turning, etc.). Yet another scenario of IoT connected devices in day-to-day life is that of how we manage our cars. As more and more devices/machines communicate with each other and systems integrate using IoT technology, a car owner would no longer miss an oil change or a service schedule of his/her car. Our true 'smart' car would preemptively reach out to our mechanic when time comes for the annual car check or say when tire pressure is sensed to be low. Our IoT connected devices (with appropriate 'apps' running on them) will throw up suggestions for car service center appointment by simply cross-referencing our electronic calendar on the device – all we need to do is just confirm a time with a one-click action. Young people busy with their work and older people with lower energy levels find 'doing grocery' a necessary but sometimes a boring task. This is how IoT would help them with that task. 'Smart refrigerators' (with sensors embedded into them) will sense when they are running low on certain items of their daily consumptions, for example, eggs or milk and will automatically populate their grocery list. Stores will also be able to push reminders to add items to their list when it predicts that they are about to be short on those items – stores will use the historical data on consumer's purchasing behavior/purchasing patterns to calculate average buying trends. When we are walking through the store, reminders will get pushed to our smart gadgets so that we avoid making another immediate trip to the grocery store just because we forgot to pick up an item or two.

Now it matters not just what is on your mind but also what is on your body – it looks like as of now wearable device technology along with IoT has possibly got the maximum attention in the IoT world. Second or third generation of IoT-based products are now being offered, with smart and attractive designs along with greater features to make those products integrate more easily with different systems. Today, we have a range of wearable IoT connectable devices ranging from products that can monitor our workout activity to those that can analyze our sleeping patterns. What is more, the devices that we 'wear' are becoming much more sophisticated, capable of connecting to all of our social media accounts and tracking much more quality and quantity data. Imagine the opportunities for uncontrolled data exchanges. Some might bring disastrous results. There are sensors that can detect and can also act on environmental and other contextual factors, such as weather, will be aware of who and how many people are around in its vicinity to change levels of input and output; and adjust to save resources and improve safety. You may like to refer to Section 29.5 of Chapter 29 where we discuss privacy considerations in the use of context-sensitive technologies.

The scenarios illustrated in this section show that the number of connected things in our lives is growing. We need to be careful what brands we chose while buying such products and how we configure them. At the same time, the sellers of those products will need to establish a trust among consumers on the personal (data) privacy front to prove that if they give up access to some of their personal data, in return they will get more tailored offers, deals and interactions rather than misuse of their collected information. Smartphones will continue to play greater role – they will be our portal into the IoT ecosystem (we already have smartphone-controlled light bulbs and cooking pots!). It is for us to decide if we wish to allow a complete remote control to our life (which probably is already the case). Organizations too need to be careful with mobile and wearable IoT connected devices to prevent malpractices. While it all sounds so glorious, the IoT does have further implications, that is, beyond the wearable devices that we use – as we shall learn during the discussion about 'Smart' Cities and 'Intelligent Buildings'.

Before reading on, readers may like to revisit or read:

Chapter 28 to understand about ***RFID technology***, ***active*** and ***passive RFID tags***, etc.

About the ***Supply Chain Management*** concept in Chapter 37 (Business Applications Security: An EAI Perspective).

Chapter 7: Security in Cloud Computing to understand the implication of ***Big Data***.

Also, see Box 10.8, Chapter 10.

BOX 10.3

Toward a 'Smart Planet': The Concept in Brief

It is said that a great evolution is taking place 'as we progress in time with technological advances. Human beings, organizations, cities, nations and man-made systems are becoming *intelligent*, *interconnected* and *instrumented*. This is expected to show us and is already showing us the ways to new savings and efficiency – perhaps equally important are the new possibilities for the 'progress' of human race. Thus, our world is becoming 'instrumented' and 'interconnected'. Almost all things, processes and ways of working are becoming INTELLIGENT.

Being Instrumented

When we say that our world is becoming 'instrumented' – it means we now have developed the ability to *measure, sense* and see the exact condition of everything and often we can do this in 'real time'. As an example, consider this:

1. There are 1 billion transistors today for each person on our planet.[1]
2. Thirty billion RFID tags have been embedded into our world and across entire ecosystems in 2010 (readers may like to visit/read Chapter 28 to understand about RFID technology, active and passive RFID tags, etc.).
3. Everything will become instrumented: our healthcare networks,[2] supply chains, cities and even natural systems like rivers.

As another example of how smart technologies can make our planet smarter, consider the case of our traffic problem. Due to the accelerating rate of urbanization, an epochal threshold was crossed in 2007 as for the first time in human history, the majority of the human population lived in cities. This urbanization is accelerating. It was predicted that by 2010, there would be 59 metropolitan areas with populations greater than 5 million – a rise of 50% as compared with 2001.

People living in larger cities are driving cars, and the products used by them are delivered in trucks. More and more cars are being poured in our roads every year – conventional approaches to managing traffic can no longer handle the world's traffic – we need 'smarter' solutions. Traffic snarls add to the cost of global economy. It will no more help merely focusing on isolated pieces of the problem, for example, widening roads, constructing new bridges, putting up more signs, creating commuter lanes, encouraging carpooling or deploying traffic copters. Time has come to look at relationships across the entire traffic system and all the other systems that are impacted by it or systems that impact traffic: 'our supply chains, our environment, our companies ... the way people and cities live and work. Traffic is not just a line of cars: it is a web of connections'.

What might the future hold? The answer is SMART PLANET! In the context of our grueling traffic problems, it is already a reality in some of the cities of the developed nations; consider this:

1. In Stockholm, using a dynamic toll system based on the flow of vehicles in and out of the city reduce traffic by 20%, resulting in 25% decrease in wait time and cut emissions by 12%.
2. Traffic controllers in Singapore receive *real-time traffic data* through sensors used to model and predict traffic scenarios; the data accuracy is 90%.
3. In Kyoto, Japan, city planners simulate large-scale traffic situations involving millions of vehicles to analyze urban traffic impact.

What makes all of this possible? The answer is an infusion of intelligence into cities' complete transportation system – a complex network of streets, bridges, intersections, signs, signals and tolls. These components can all be interconnected and made 'smarter', that is, much more efficient and less energy consuming; energy shortage is one of our glaring problem on the planet earth. 'Smart Traffic Systems' can improve drivers' commutes, supply better, that is, dependable information to city planners and enhance the productivity of businesses and raise citizens' quality of life. They can reduce traffic congestion, bring down fuel use and reduce the emission of CO_2.

Being Interconnected

When we say that our world is becoming 'interconnected' – it means people, systems and objects have the capability to communicate and interact with each other in unconventional ways. Note this:

1. There is already 1 billion strong Internet of people. By the end of 2011, almost one-third of the world's population was on the web.[3]
2. There are more than 4 billion mobile phone subscribers worldwide.[4]
3. The IoT involves appliances, cameras, cars and motorways, network of pipelines, pharmaceuticals and even livestock – it is headed to become a 1 trillion figure!

X 10.3
ntinued)

Being Intelligent

When we say that our world is becoming 'intelligent', it means our ability to respond to changes *quickly* and accurately (today's era belongs to 'business at the speed of thought' – remember the epoch-making book by Microsoft's Bill Gates), and our ability to fetch better results by predicting and optimizing for future events. Note this:

1. There is BIG Data: 15 petabytes of new information are being generated every day. This is 8x more than the information in all the libraries of the United States.
2. An average company with the size of 1000 employees spends $5.3 million a year to find the information stored on its servers.

New computing models are emerging to handle, analyze and manage the enormous amounts of data generated as a result of the proliferation of end-user devices, actuators and sensors. This is combined with advanced analytics (i.e., Business Intelligence). These technologies are making us smarter. What does the future hold? The answer is **SMARTER Planet!** Figure 10.5 puts it all together.

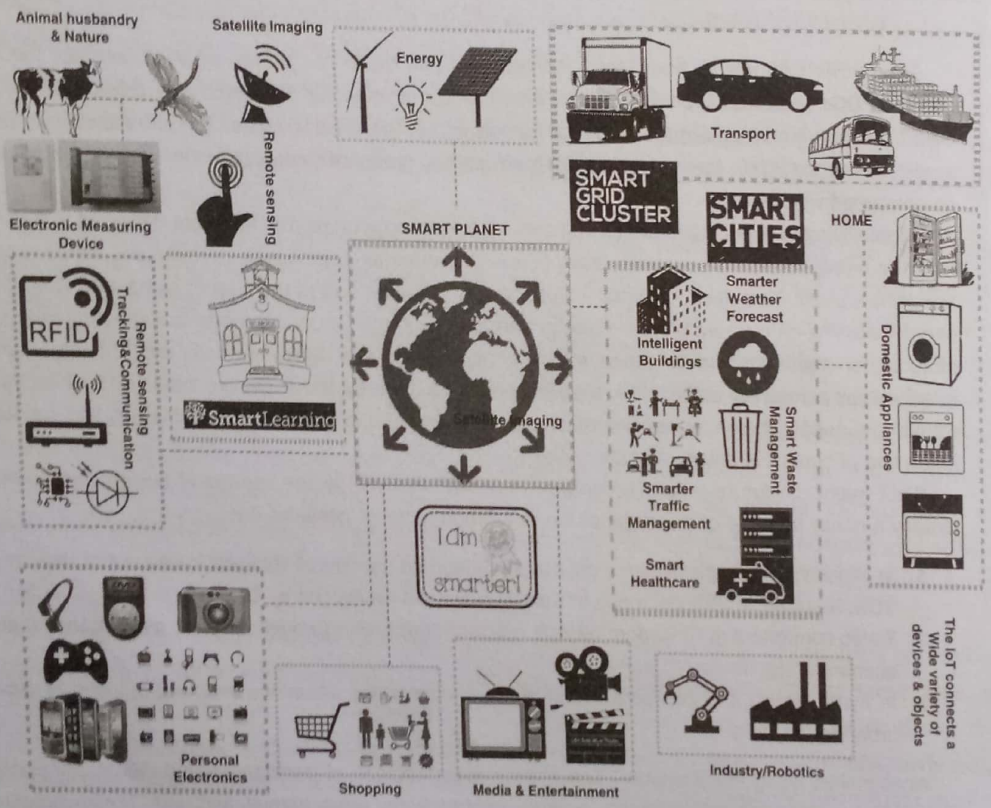


FIGURE 10.6 | Smarter planet: Putting it all together.

10.3 Understanding Security and Privacy Issues in IoT

Figure 10.7 presents the technology roadmap of the IoT. Note the various technological milestones depicted in that diagram. As regards the software agents mentioned there, there are several privacy issues surrounding them; those are discussed in Chapter 28 (Section 28.7.6). In the same chapter, there is a discussion about RFID technology and its related issues. A point worth noting in Figure 10.6 (IoT Roadmap) is the increasing technological reach of each successive wave of the IoT and its increasing capability. As an example of this scenario in the domain of agriculture, imagine a sprinkler system that is not on its own but rather makes use of weather forecasts, weather sensors and also connects to the 'services' available through the consumption model based on pay-by-use water rates. This way, the sprinkler working in IoT will be able to optimize the watering of your lawn. In the world of 'smart cities', one could imagine a public trash collector that has the mechanism to compact the garbage inside it as needed and then it can alert the garbage cleaners in the city workers when it is full to get it collected rather than the cleaning workers coming to the garbage cans every morning. Of course as yet, this may sound like a dream for the heavily populated cities in the developing countries like India.

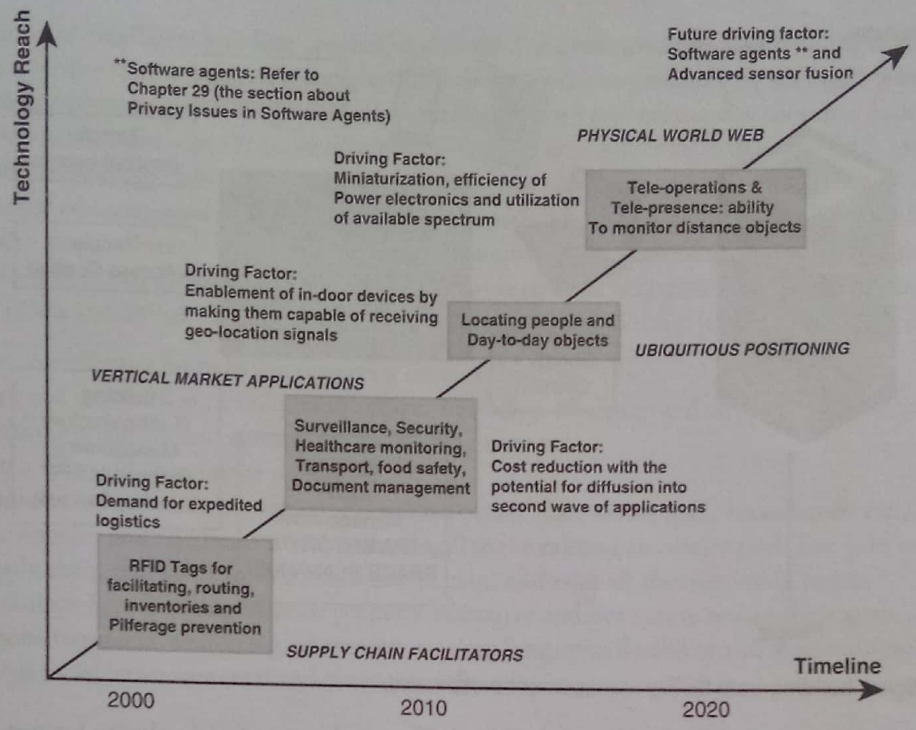


FIGURE 10.7 | The IoT roadmap.

The concept of IoT (refer to Section 10.2) sounds so wonderful; it sounds almost like a Sci-Fi. Naturally, one wonders if there could be a downside to it and that indeed is so. As explained in Chapter 27, *privacy* is a fundamental concern in the modern day. The very fact that the devices are part of the IoT exchange so much information, one can imagine the privacy issues arising in the scenario. We discuss those issues in the remaining sections of this chapter.

Before reading on, readers may like to revisit or read **Chapter 27** to get the foundation on the *fundamental privacy concepts*.

Smart home devices, connected cars and wearables, that is, wearable digital devices collect vast amounts of data about things relating to their owners/users. This makes many people worried about the potential risk of personal data getting into the wrong hands. Number of access points on the rise also poses a security risk. What is more, now there are also cooking vessels available that can be controlled using our smartphones! You can see one such demo at the URL (http://recode.net/2014/07/24/belkins-smartphone-controlled-crock-pot-doesnt-dish-enough-features/). Even though the idea of IoT may be good and the fact that it probably existed for years, it is only now that the IoT has entered the consumer space. However, the usage of IoT is yet to mature. Both good and bad IoT services exist and it is for us to decide which one we choose and how cautious we can be; protection and prevention is in our hand. Therefore, it is always a good idea to take up product research, also a good idea to always buy from a company you trust, and making sure you are getting a solution that is actually meant for the resolution of your problem.

10.4 Intelligent Buildings: Security Threats

'Intelligent Building': The Concept

These days, we hear a lot about 'intelligent buildings'; however, the concept is not new. When you look at a modern building from outside, it may not shout 'intelligence'. It is the integrated technologies built inside the building that make it 'smart'. Consumer technologies play an important role in 'intelligent' buildings. IoT enables smart buildings to reap the benefits of web-enabled technologies. These technologies are used for managing various needs of a building, for example, lighting, ventilation, heat and elevators; see Figure 10.8.

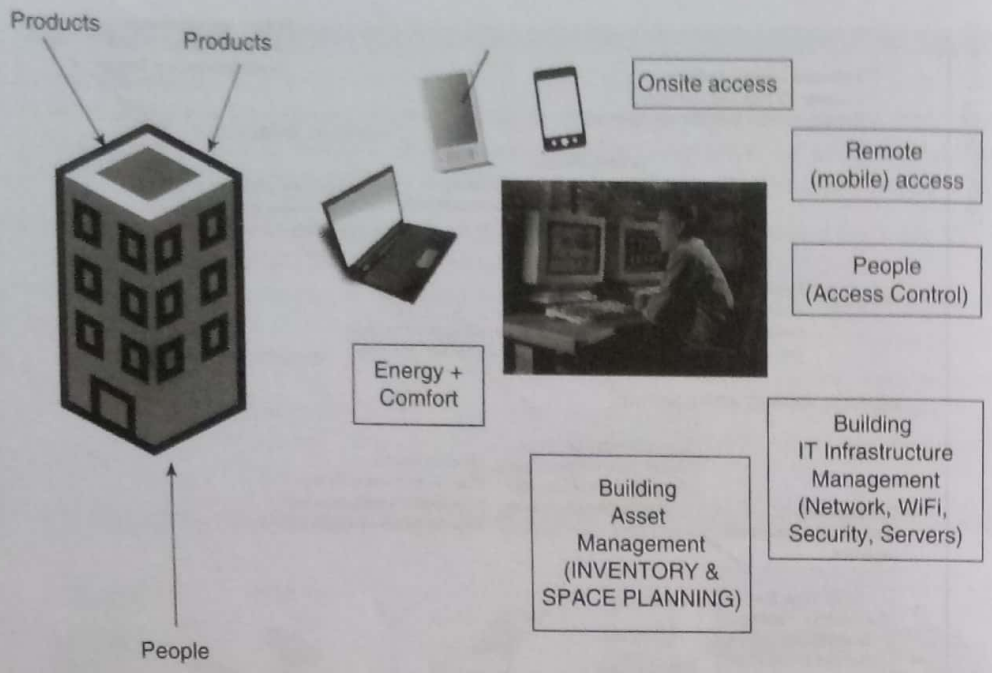


FIGURE 10.8 | Intelligent building from facility management perspective.

Let us understand what we mean by 'intelligent building'. They make use of technologies for not only improving the building environment and functionality for occupants/tenants but also for controlling costs, improving security, comfort and accessibility and also for improving 'energy efficiency'. Seen another way, an intelligent building is one that provides a productive and cost-effective environment based on a triple P concept (i.e., PPP). It is based on the three basic elements: (1) *People* (services users/facilities management), (2) *Products* (structure and facilities provided) and (3) *Processes* (automation, control, systems, maintenance and performance) and the inter-relationships between them (see Figure 10.6), PPP concept of *intelligent building* and how it looks to its operators, that is, facility managers of 'intelligent buildings'. Also, see Figure 10.9.

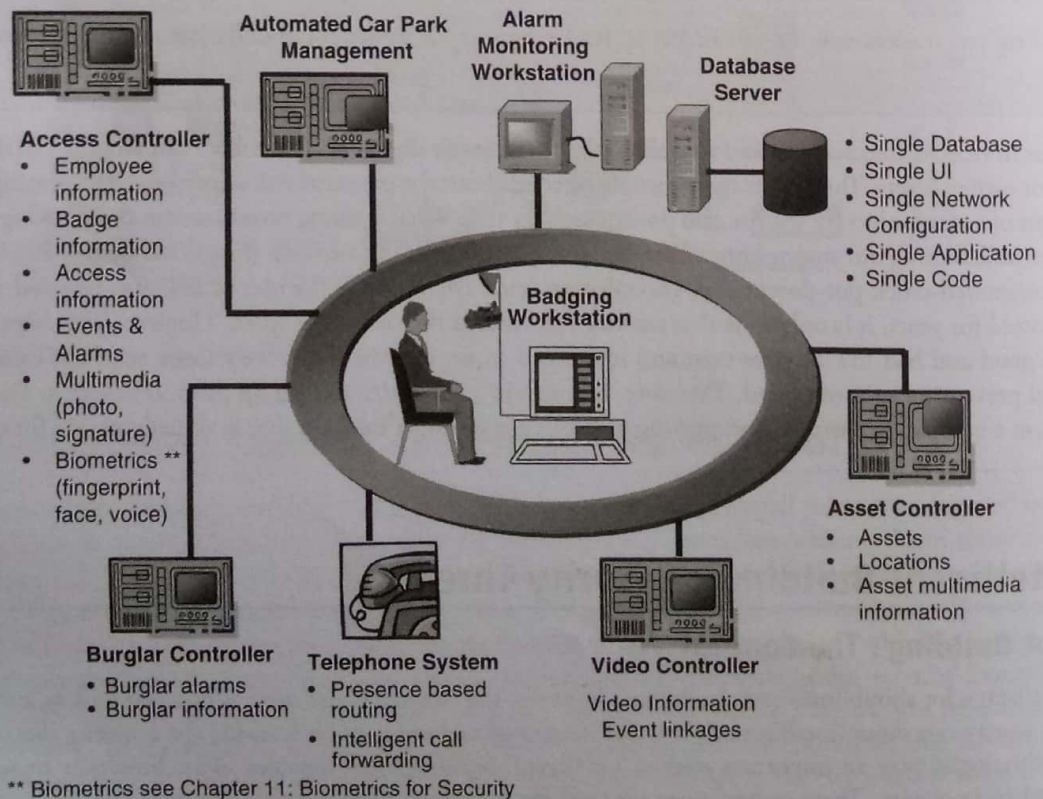


FIGURE 10.9 | Support systems for intelligent buildings.

A complete definition of 'intelligent building' touches upon several of its dimensions: (1) a building that uses both *technology* and *process* to create a facility that is *safe*, *healthy* and *comfortable* and enables productivity and well-being for its occupants, (2) an intelligent building provides *timely, integrated system information* for its owners so that they may make *intelligent decisions* regarding its *operation and maintenance*, (3) an intelligent building has an implicit logic that effectively evolves with changing user requirements and technology, ensuring *continued and improved intelligent operation*, *maintenance* and *optimization*. It exhibits key attributes of *environmental sustainability* to benefit present and future generations. Note that the definition takes into consideration the green aspects, that is, environmental sustainability. According to IBM, *Smarter Buildings* are well managed, integrated physical and digital infrastructures that provide optimal occupancy services in a *reliable*, *cost-effective* and *sustainable* manner. IBM's concept of 'Smart Buildings' indicates that such buildings have the following characteristics:

1. They are more cost-effective by reducing operating costs and energy.
2. They use active and designed-in techniques to achieve reliability, efficiency and environmental responsibility.
3. The provide visibility, control and automation to building systems.
4. They maintain a safer and more *secure workplace*.
5. They communicate in real-time to supporting infrastructure (i.e., smart grid, broadband, etc.). Smart grid means adding ICT (computer and communications technology) to the existing electricity grid. The 'grid' refers to an enhanced electricity supply chain that starts from a major power plant and ends all the way inside homes.
6. Intelligent Buildings help building owners, property managers and occupants realize their goals in the areas of costs, lifetime energy management, well-being, convenience, safety, long-term flexibility and marketability to achieve buildings which have high social, environmental and economic values.

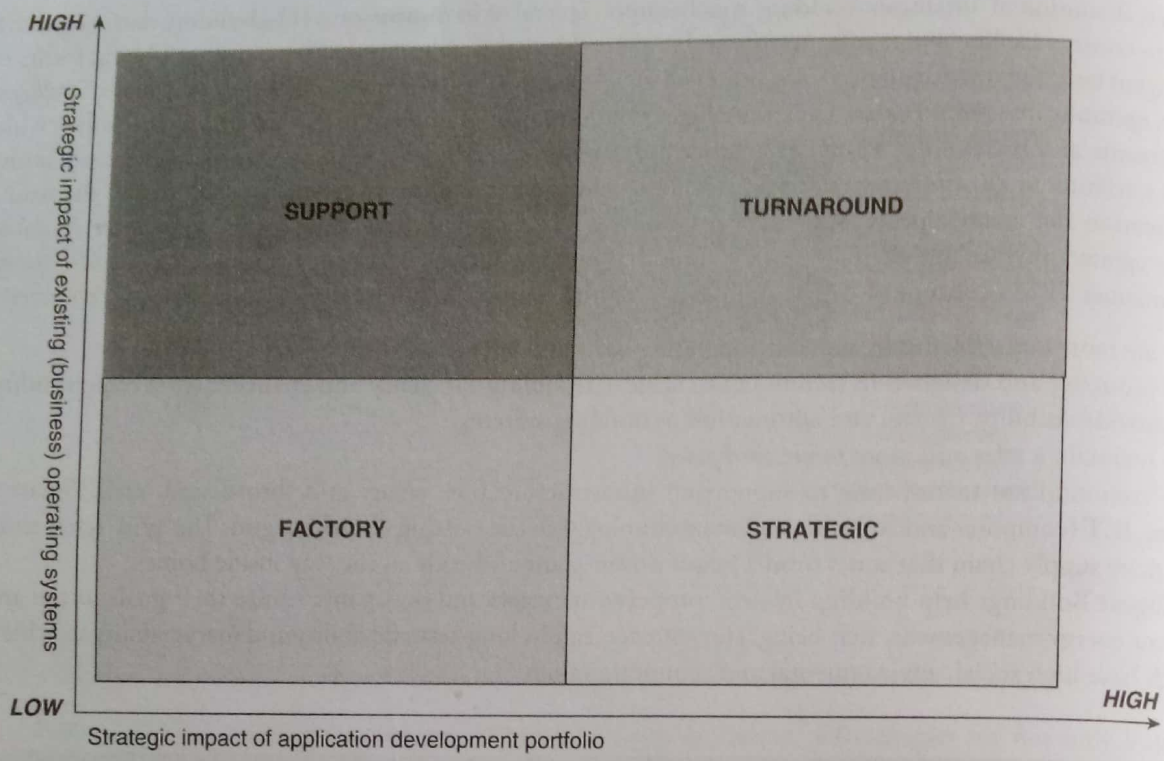
BOX 10.4

Intelligent Building: What Is It?

We may not find a precise definition for an 'intelligent building'; however, a common theme is the one that centers on 'integration of technologies'. For the purpose of this chapter, we agree to understand an intelligent building as one wherein there is a combination of technologies and interconnected systems to support the use of the accommodation by those who use, run and/or occupy the building and the combination of technologies enable the efficient operation of the building and also enables reconfiguration of the space in response to changing use, that is, the 'churn'. Some people also use the term 'smart buildings' to refer to intelligent buildings. The systems which may be integrated are mentioned below:

1. **Building Systems**
2. **ICT (Information and Communication Technology) Systems**
   - Building management system
   - Office automation (e-mail, data and Internet)
   - HVAC controls and Access control
   - Media/multimedia (voice, video, music)
   - Lighting control and Intruder alarm
   - Telephony (voice, fax, videoconferencing, SMS and pagers)
   - Security/CCTV and Fire alarm IP-based applications
   - Water management
   - Waste management utilities and Stand-by generators/UPS
3. **Business Systems**
   - Enterprise resource planning
   - Material requirements planning
   - Customer relationship management
   - Integrated command and control center
   - Integrated service/helpdesks

As a conceptual foundation to understand the impact of and dependence on IT systems in modern life, refer to Figure 10.10. For IT applications, there are two dimensions of the impact: (1) the impact of application development portfolio and (2) the impact on existing business operating system. Similarly, for information technology (IT)-enabled 'intelligent buildings' also the impact for the applications developed for it will have these dimensions.



Strategic grid (source: McFarlanand McKenney)

FIGURE 10.10 | The strategic grid of IT applications.

Key Features/Characteristics of 'Intelligent Buildings'

In addition to those already mentioned, intelligent buildings also possess the aspects listed below:

1. They are designed around the needs of their inhabitants.
2. They are supposed to improve *Security.*
3. They provide enhanced comfort to people living in them.
4. They result in *Energy Savings.*
5. They are capable of *Energy Monitoring.*
6. Devices in the building and those of the users in the buildings communicate based on the IoT.
7. They provide (1) *Local Command and Control* and (2) *Remote Command and Control.*
8. Dwellers of the building have the *Access to information from anywhere.*
9. They enable getting the right data to the right people.
10. They *Add Value.*

Today's environmental pressures have created the need for efficient and cost-effective use of the built environment. It is also driven by the need for economic efficiency. We need buildings with a lower cost of ownership. Intelligent buildings are supposed to be a solution toward this – see Figure 10.11.

Note the mention of 'smart grid' in Figure 10.11– a smart grid works based on an intelligent monitoring system which is used to keep track of all electricity flowing in the system. A smart grid is a complete overhaul of electric transmission and distribution. Systems must fulfill the need of twenty-first century infrastructure metering. Modern technologies such as wireless communication, geographical information systems, etc., are effectively used in 'smart grid' to improve the methods delivery and use of electricity. There are four main components of a 'smart grid', namely (1) advanced asset management, (2) *advanced metering infrastructure,* (3) advanced distribution operations and (4) advanced transmission operations. Each component has

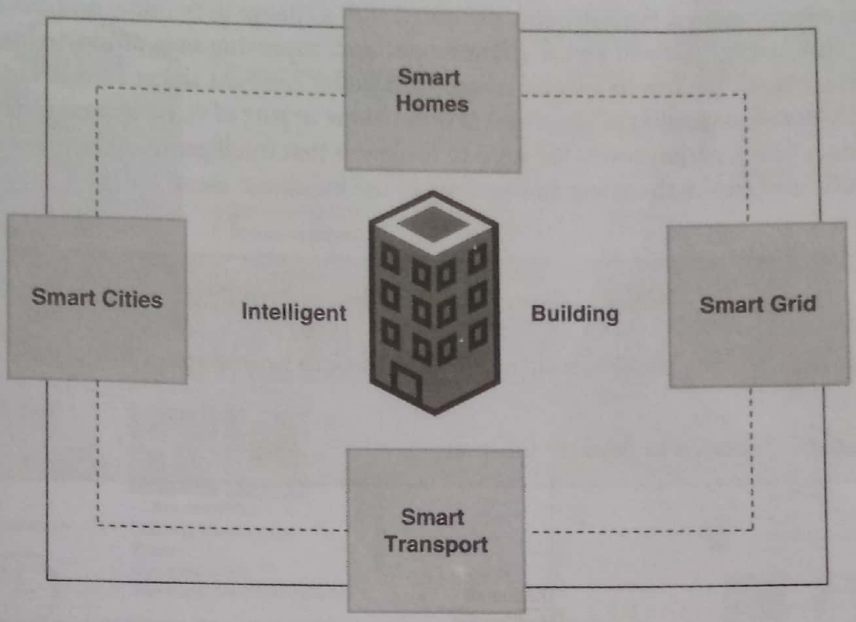


FIGURE 10.11 | Intelligent buildings.

a role to play, for example, a direct two-way communication between a utility and the customer will be established using the advanced metering infrastructure. This will provide a variety of information, such as real-time pricing and usage information over certain time periods. The advanced meters will enable 'green' buildings in the sense that they will enable customers to respond to real-time electricity prices toward better management, monitoring and control of *energy use* in their homes. Consciousness about electricity usage is indeed the need of the hour given the phenomenal rise in the consumer electronics in the past few years. Modern homes have high-definition televisions, computers and video game systems – they all consume electricity. While people enjoy the advancements in consumer electronics, they need to keep in mind the environmental impact due to high energy usage; this is where the smart grid is expected to help. While the concept is good, there are some security concerns that need to be addressed for intelligent buildings. Let us consider the case of 'smart grid'. This is one area where the threat is from malicious software which is fully recognized and it is especially relevant to the intelligent building. Malicious software can infect the electricity plant controllers that intelligent buildings use. It is a pity that attention to physical security (refer to the chapters on this topic available on the CD companion of this book) is receiving less attention as compared to network security. Proponents of intelligent buildings concept might require some convincing that cyber threat indeed is a potential threat area for these high-tech buildings. It may be easier to convince power engineers about this threat as they hold a much higher awareness level because they do experience the impact of malfunctioning control software. Some world incidents show that 'successful' malicious software could shut the whole system down for weeks. It is estimated that the business for cyber security on the smart grid is around $21B over the next 5 years. Software running on open systems (such as the Windows operating system, for example) always is more prone to cyber-attack! This is because an open software platform can only be protected from malicious software that has been identified, but not against malicious software yet to be deployed. After all, it is the operator who defines 'malicious' not the machine! Almost all virus protection services provide security against known, that is, characterized risks with identifiable signatures. Hence, there can be at least one user who would be closing the stable after the horse has run away! Smart grids use programmable logic controllers (PLCs) – the compiled code in a programmable controller is usually not too easy to interpret; with some efforts, it is possible to reduce the ability to tamper with it. Therefore, cyber attackers aiming to bring the smart grid down are likely to be focused on the system characteristics of the objects into which the code is bundled, for example, buffer overflow, which is typically provided in sources such as system manuals or sometimes they are exposed on the web. Security risks are associated with 'intelligent buildings' and are further discussed in the next section.

Intelligent Buildings and Security Risks

Security should be an essential design element for intelligent buildings and not an afterthought. Figure 10.12shows the generic threat profile as well as the relation between threat, exposure and risk as well as other elements related to security. The concepts explained in Section 2.6 (Classification of Threats and Assessing Damages) of Chapter 2 and Section 5.12 (Event Classification) of Chapter 5 are applicable to the security of intelligent buildings too. On one hand, intelligent building present

benefits such as potential energy savings, the lesser cost associated with a change in building occupancy and configuration (i.e., churn), maintaining a comfortable, safe and secure environment and improving user productivity, on the other hand, they open new fronts for cyber-attacks! We live in a world where IT is under constant threat from a variety of sources. Therefore, an IT system is potentially at risk, regardless of whether it is stand-alone or part of an integrated system means the deployment of these innovative solutions is not without risk. We need to recognize that intelligent buildings are complex systems and put in place appropriate practices to ensure the safety and security of the buildings' users.

Physical Security of 'Intelligent Buildings'

It is important to keep in mind that 'physical security' will continue to be important in the days of a modern high-tech era.

Physical security aspects are discussed in detail in Chapter 35.

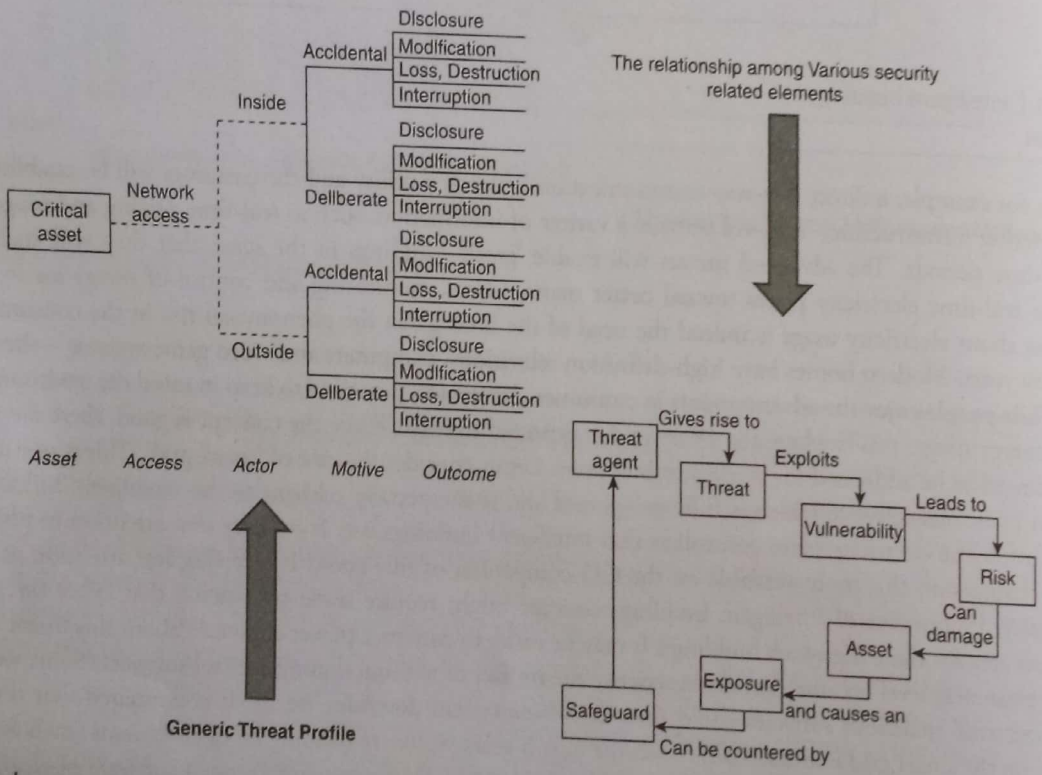


FIGURE 10.12 | Generic threat profile and threat, exposure and risk.

Let us consider some examples in the realm of 'intelligent buildings' – the first example is that of modern office environments. Over the past few years, an increasing convergence of infrastructure has been seen in the office environment. Economic pressures drive office systems to operate the accommodation efficiently – one can see such scenarios especially in metropolitan cities. Depending on the objectives of the building owners, operators and occupiers, the level of convergence achieved varies considerably. Figure 10.13 illustrates the wide range of systems that are now typically managed over an IP-based infrastructure.

Today, the economic and environmental pressures for greater operating efficiencies have led to increasing convergence of infrastructure, both from end-user perspective as well as from energy efficiency standpoint. Depending on the objectives of those who own the office building and those who operate, that is, manage those buildings, as mentioned before, the levels of convergence achieved with various technologies varies (e.g., IT, Wi-Fi environment usage and IoT). In modern buildings, where intelligent buildings are going to occupy a central part, the trend is to make use of a common centralized building management system (BMS) for the purpose of controlling the individual building systems. This is a vast change from the traditionally used practices for managing building services. In the past, people used different building systems (e.g., HVAC,

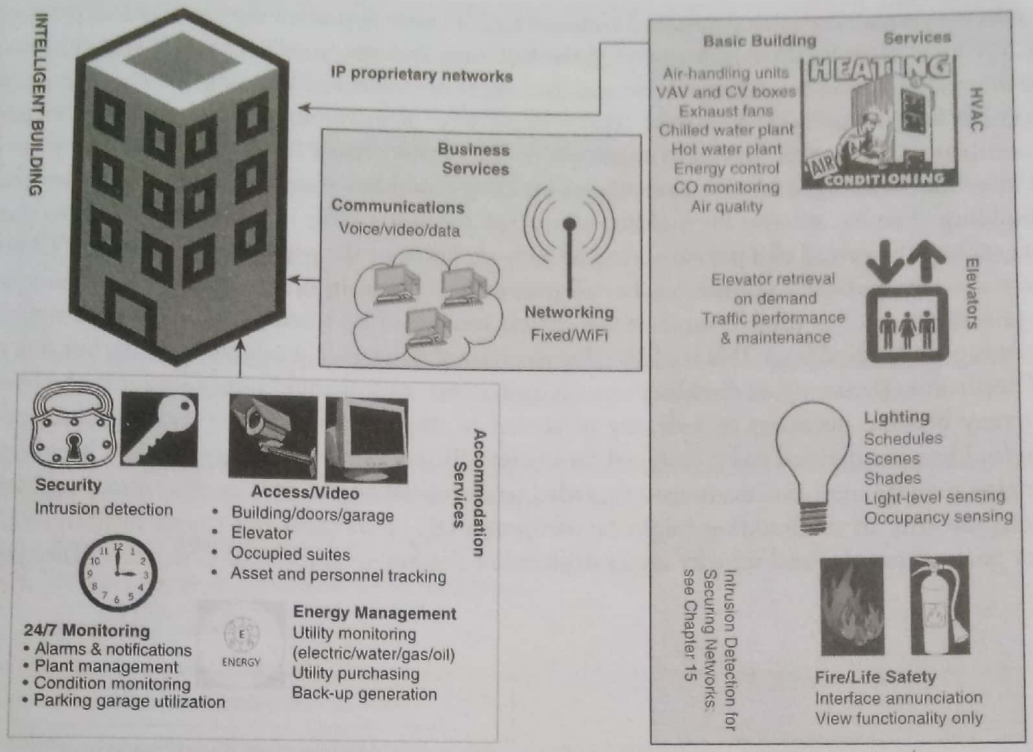


FIGURE 10.13 | Proprietary networks in intelligent buildings.

CCTV, access control, lighting, energy management, etc., see Figure 10.13). Each system would have their own control, and often for their implementation disparate methods of cabling would be used. Movement of these systems onto a common cabling and TCP/IP-based network infrastructure is the first step in the convergence process; however, in such a scenario, though efficient from an operational perspective, all the potential threats to TCP/IP-based networks are applicable to the networks used in intelligent buildings also. Adoption of such integrated systems for the architecture intelligent building allows the implementation of central control facilities via a singlebrowser-based operator interface. As we know web-based applications do have security threats. While a centralized BMS permits the remote monitoring of the facility via the Internet, this very dependence on the Internet opens new attack opportunities for intruders; add to this the fact that people in intelligent buildings would most likely use IoT connected devices.

The very nature of intelligent buildings (refer to Figure 10.11) becomes the breeding ground for security attacks on them. First, given that such buildings greatly depend on its converged infrastructure – see Figure 10.13, it shows the proprietary networks in intelligent buildings. Integration of basic building systems with its supporting business systems (see Box 10.4) potentially creates a range of new risks associated with aspects of the personnel, technology and operations. At the greatest risk potentially are the human elements of the building operations – this is because, whether accidentally or deliberately, individuals may tend to bypass security controls or may operate the building systems incorrectly or there could be bugs in the software designed for the building systems. The integration of systems can amplify the impact of errors or omissions. Systems integration means teaming facilities management professionals with IT professionals – these two groups often have different priorities, cultures and also their reporting chains may not be the same. All of these can prevent an effective response to incidents or faults. Seen from a technology standpoint, integration may introduce new failure modes, where building systems can create interferences with business systems and vice versa.

Intelligent Buildings and Cyber Security

Cyber security is also an issue with an intelligent building that uses a high degree of ICT integration.

Author's book titled *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives* (Wiley India, isbn: 978-81-265-2179-1) is the recommended source for gaining insight into how cyber-attacks take place.

As far as security is concerned, the critical issues to consider are: (1) how to protect the security and privacy of a building's owners and users, (2) how to maintain the integrity of the building and operations within it and (3) how to ensure the continuing availability of the accommodation for owners and users of intelligent buildings. When the convergence of the technical infrastructures and integration of systems creates unplanned or unauthorized pathways, the security and privacy of the building's occupants and owners may be compromised. This would result in unauthorized access to systems or loss of data (to get an idea what possibly 'data' of an intelligent building could be – refer to Box 10.4). As an example, consider this – intelligent building often has systems for building access and room-booking; unauthorized access to these systems may reveal personal data such as the period of a person's being away from home or the presence of a visiting VIP, etc. The integrity of the building may also come under compromise if third parties gain access to or control of critical building systems. If a third party could gain the control to disable some of the critical systems of an intelligent building it might not be safe any longer to continue being in that building. This could be due to physical damage (e.g., flooding or fire) or due to threats to the health and lives of occupants. Bypassing or disabling security and access control could put in jeopardy the lives of inhabitants of the building. It may become necessary to redeploy personnel to implement manual checks in place of the automated systems. Intelligent building is supposed to be designed for energy efficiency and for energy-efficient buildings. Hence, if the operation of the energy management functions were degraded or disrupted by the actions of a third party, whether by direct manual intervention, integrity of the building might be compromised – remember the tripod diagram – C.I.A. (the three pillars of security or goals of security and security layers depicted in Figures 4.1and 4.2 of Chapter 4. They are reproduced in Figure 10.14).

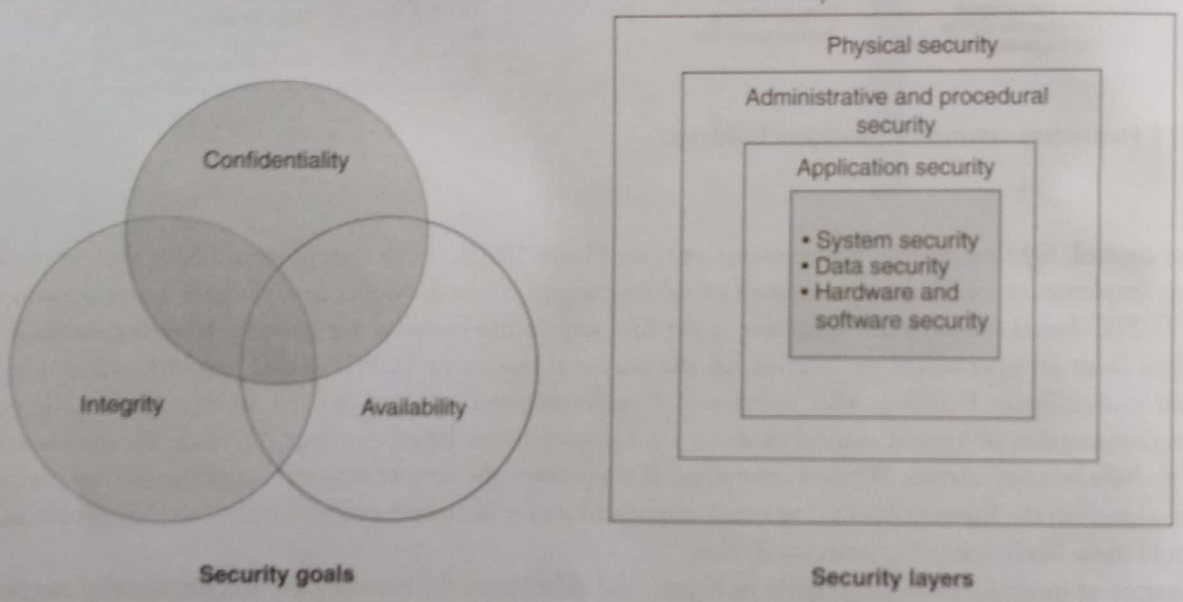


FIGURE 10.14 | Security goals and security layers.

Interference with the security of intelligent building's critical system or the deployment of malware will result in compromise to the security of the building. The 'availability' (see Figure 10.13) of the building may be seriously affected when building systems are disrupted (implications of disruptions in business operations are discussed in Chapter 31), thus preventing the building from delivering the required functionality. The nature of the availability risk will depend on the type of building and the criticality of the affected building service. As an example, when a BMS cannot be operated and thus allows the temperature to go astray, that is, it goes outside acceptable limits, the building may no longer become comfortable from occupation standpoint for its dwellers, and equipment may get damaged if there are excessive temperatures, or may cause damage to stored materials. In high-rise buildings, interruption to the operation of vertical transport systems (i.e., lifts and escalators) could seriously affect the availability of upper areas if occupants are no longer in a position to use the stairs or unwilling to use them.

In the domain of sports, stadiums play a pivotal role; Figure 10.15 presents some typical IP-based systems in modern stadiums which are also a part of 'intelligent' buildings – we can get an idea of the technological and other types of

BOX 10.5

Key Terms Relevant to Intelligent Buildings

Bluetooth: A wireless technology standard [IEEE 802.15.1] used for communicating data over short distances and which may be used to create personal area networks.

Continuity: The unbroken and consistent operation of a system, process or business over a period of time(refer to Chapter 31).

Convergence: The tendency for previously separated technologies, for example, voice, data, video, to now share resources, both physical (e.g., cabling) and logical (processing, storage, etc.), and to interact with each other (refer to Chapter 7).

DMZ: Demilitarized zone – a physical or logical sub-network protected by firewalls used to share data between trusted and un-trusted networks, for example, between an organization's intranet and the Internet (refer to Section 16.3 of Chapter 16).

Governance: The management, decision-making and leadership processes employed by an organization to ensure consistent and cohesive management of a given area of responsibility.

HVAC: Heating ventilation and air conditioning.

ICT: Information and communications technology.

ICS: Industrial Control Systems

Malware: Malicious software used to attack, disrupt and compromise security, or take control of a computer system or individual computer (refer to Chapter 6).

Resilience: The ability to withstand a level of failure or disruption and to adapt or respond to dynamic internal or external changes while continuing to operate with limited impact on the organization or business (refer to Chapter 31).

RFID: Radio frequency identification (refer to Chapter 28).

SCADA: Supervision Control And Data Acquisition.

Structured Cabling: The implementation of a structured building or campus telecommunications (i.e., telephony, computer network, video, etc.) cabling infrastructure, which comprises a number of standardized smaller elements.

UPS: Uninterruptible power supply – an emergency power system providing continuity of supply in the event of an interruption in the mains power supply.

Wi-Fi: Technology used to deliver a wireless local network based on the IEEE 802.11 standards.

ZigBee: A specification for a communications protocol using small, low-power digital radios, based on the IEEE802.11 standard for personal area networks (see Box 10.2).

complexities involved in modern stadiums designed to provide *business services* as well as *building services*. Looking at IP-based systems present in modern stadiums (see Figure 10.14), we realize that modern sport stadiums are almost like a large town or small city – they contain a plethora of services and devices; including BMS heating, CCTV and public-address systems heating and air conditioning and air ventilation systems, security monitoring systems, lighting, fire, operating systems for lifts, escalators, digital electronics for the scoreboards, telephones, Internet access for press and visitors, integration with business systems (e.g., supply chain and payroll), electronic point of sale, ticketing and turnstile systems. When sports events are hosted, there is also a demand for access to large-format video, master aerial television and broadcast systems.

As we have learned so far, looking at the office environment in intelligent buildings and modern sports stadium, a number of technologies and smart devices (some of which are IoT connected) are used in those buildings – this does pose some 'interoperability' issues because systems and devices from multiple vendors often do not play together well although there are mature standards for inter-accessibility. This may happen although standard protocols (some explained in Box 10.1 are supposed to allow easy multi-vendor interoperability). Often, due to so-called 'business reasons', vendors tend to 'lock-down' even devices that are designed to

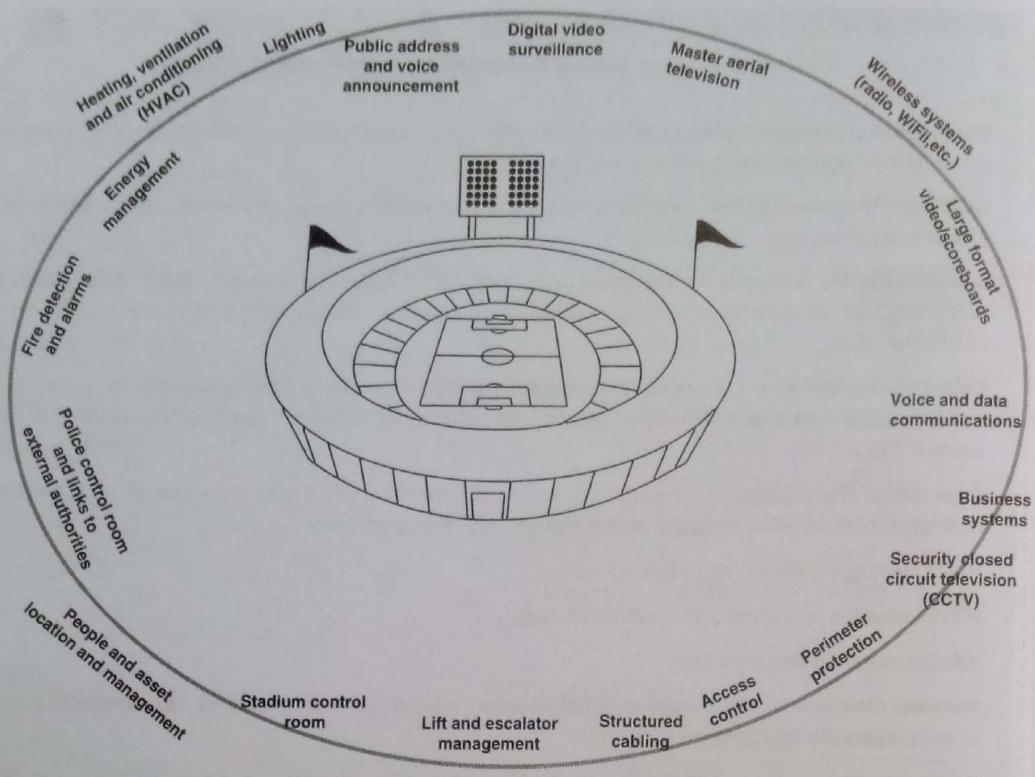


FIGURE 10.15 | Modern sports stadium: IP-based systems.

use standard protocols; the motivation for this could possibly be their ambition to gain a dominant position in the market. Thus, to conclude, most automation system for intelligent buildings that have extensive technology integration and Internet control may end up becoming proprietary as far as the connectivity protocols are concerned.

Security Best Practices for Intelligent Buildings

As mentioned in the previous section, intelligent buildings could pose security risksto people living inside such buildings. This is so because the security of BMS of an intelligent building is a relatively new area in most parts of the world. Once upon a time, the BMS used to be a stand-alone system based on proprietary controls. However, now with the emergence of the IoT, there is a growing trend toward interoperability among the systems and devices used in the intelligent building. Many proprietary technologies are getting phased out to bring in industry standard solutions and this has resulted in quite a lot of growth in the use of open protocols. These open protocols sometimes can be the root of security attacks on intelligent buildings. While these innovations in protocols may offer benefits to the integration of building management systems, their use indeed requires security assessment. To mitigate the security risks, application of best practices is essential for securing intelligent buildings. Figure 10.16 is the schematic representation of the architecture diagram for the network infrastructure of an intelligent BMS (iBMS).

A number of best security practices for intelligent buildings are mentioned below:

1. **Physical security:** There is no substitute for physical security and no security plan is complete without it. We need physical security to prevent unauthorized access to the devices used in iBMS (see Figure 10.14) such as networks and information. Without physical security, intruders would have the means to circumvent all other methods of protection. Combining multiple barriers to access, places such as building, room and cabinet, control is a good practice from a physical security perspective. It is also essential to locate mission-critical devices in access controlled areas or in locked cabinets. Preventing unauthorized physical access to network devices such as routers, firewalls and switches is also a must. Another good practice is to protect communication cable runs with conduit or ruggedized cable chases.
2. **Network infrastructure deployed in intelligent buildings:** The network is the medium through which information to flow across the components of an integrated building management system and the outside world. If intruders are able to

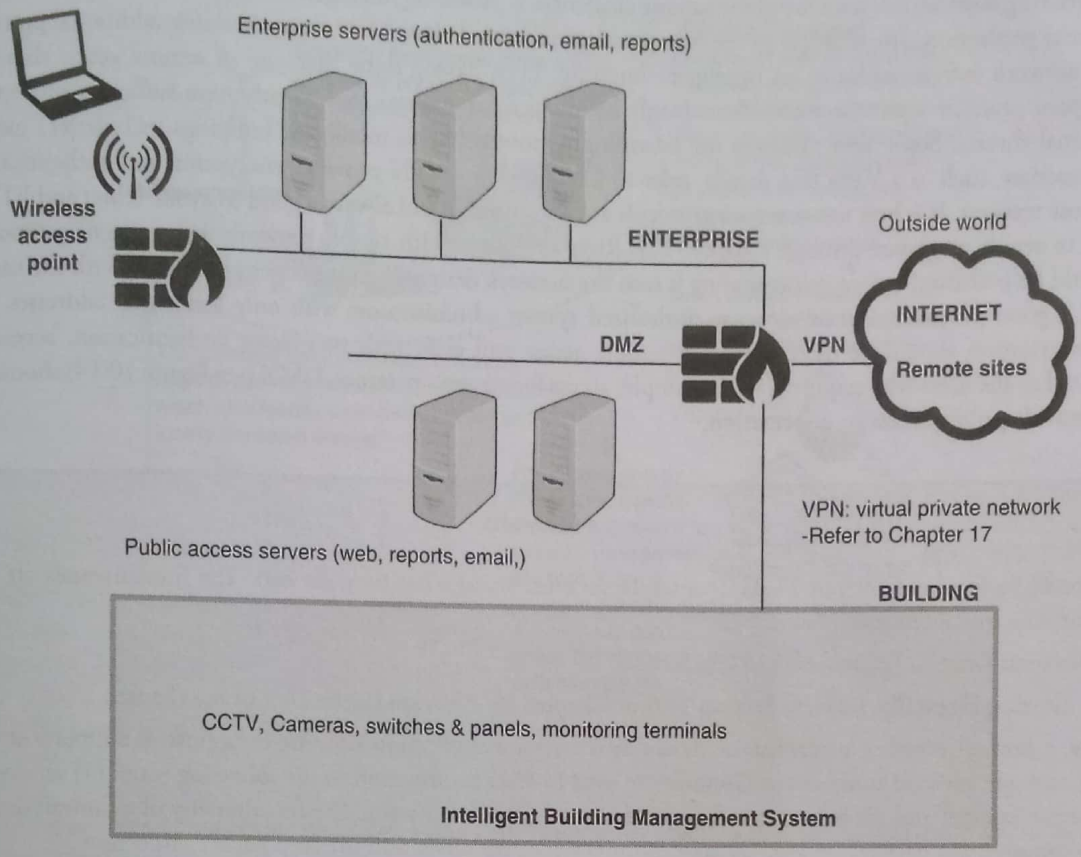


FIGURE 10.16 | Network infrastructure of an iBMS.

tap into the network, they can disturb the flow of information; therefore, it is best to isolate iBMS as much as possible. Locate it on a virtual local area network (VLAN) server to ensure that building traffic, including broadcasts to all nodes, remains within the logical boundary established. Careful thinking is essential before outside access is granted. Each point for entry to and exit from network must be secured. The risk is minimized and security costs can be kept down by granting access on a need-to-know basis ,that is, granting access only when a valid reason exists.

3. **Controlled access through the use of Firewalls:** Firewalls are explained in Chapter 16 (Firewalls for Network Protection). They contribute to security by controlling the flow of information into and out of the network entry points. Using user-defined configuration rules rather than using the default security settings for the firewall is a good security practice. A firewall determines which traffic will be allowed to pass through and onto the network. Traffic that is not compliant with the configured rules is rejected. A single best practice applies to adding firewalls to the network design of the intelligent building: a firewall should be placed at every transition point into or out of the intelligent BMS network. Proper selection and placement of firewalls is a rigorous effort and is beyond the scope of discussion in this chapter.
4. **Managing user access:** Use of authentication and authorization for secure user access is the basic tenet of security. Authentication is nothing but the means by which a user's identity is established – basic principles of authentication are explained in Section 11.2 of Chapter 11). Once authenticated, a user is authorized to perform certain functions commensurate with their role defined in the access control table. As part of security practice in intelligent buildings, user access should be restricted based on practices commonly deployed by IT departments, such as, central authorization, password control, user access management and network monitoring. Further user access restriction can be achieved by establishing authorization requirements for individual devices such as routers, servers, embedded controllers and workstations. The best approach is always dictated by the type of devices used. As a best practice, it is good to consider stronger authentication methods for critical host devices such as smart cards or USB tokens. As explained in Chapter 11, biometric authentication helps to limit access based on a physical or behavioral characteristic such as a fingerprint. Two-factor authentication helps to limit access to users that requires both a password and a physical token.

5. **Restricting Remote Access:** One of the unique challenges is providing intelligent BMS access to remote users. Additional security protections (in addition to the best practices presented above) – it means building additional protections into the network infrastructure of an intelligent building. Even having done that, use of remote access should not be a rampant practice – remote access should only be allowed for systems that already have sufficient protection against external threats. Some best practices for providing remote access to intelligent buildings include: (1) using a secure connection, such as a VPN (for details, refer to Chapter 17) – VPN provides encryption and authentication during remote sessions. It is best to use secure protocols as far as possible and always a good to avoid Telnet and FTP (you may like to revisit or glance through Chapter 12). Risks associated with simple network management protocol (SNMP) should be evaluated before incorporating it into the network design of an intelligent building. With the use of SNMP, it is a good practice to limit access to authorized system administrators with only known IP addresses. Two-factor authentication should be used to restrict remote access and even with two-factor authentication, access should be limited to the users who require it – for example, access for system operators. DMZ (see Figure 10.14) should be created to provide public access to information.

Firewalls

For Firewall basics – see Section 16.2, Chapter 16 to understand what firewalls are). The fundamentals are available below for your quick reference:

Proxy Servers: Refer to Section 16.5 of Chapter 16.

Packet-filtering Firewalls: Refer to Section 16.6 of Chapter 16. Also, see Figure 16.4 of the chapter.

Basically, a firewall is either a stand-alone device or a software application running on a host. It supports at least one internal and one external connection. Firewalls are used to filter information in the following ways: (1) service control, (2) direction control and (3) behavior and content control (email and web). The functionality of a firewall ranges from basic to complex: (1) packet filtering, (2) application level: proxy server and (3) deep packet inspection.

Setting up of firewalls is an important area of IT support; it requires special expertise for appropriate selection and configuration of firewalls.

'Intelligent buildings' are rapidly becoming part of 'smart cities' – a phenomenon discussed in the next section.

10.5 Smart Cities: Privacy and Security

Most large cities in the world are facing problems such as energy crisis, climate change, overpopulation, changing demographics, coping with technological impacts, increasing expectations from empowered consumers, deterioration of city infrastructures, fund shortages, increasing pressure on supply chains, deterioration of the environment, that is, pollution. At the same time, data and information, not only about machines, devices but also of human beings, is being exchanged like never before. In fact, the convergence of video, text, sound, as well as other forms of digital data, has resulted in 'BIG data' (refer to Chapter 7). We are making technological advances to become a 'smart planet'. Leading organizations such as IBM have done pioneering work in this regard. Let us understand the concept of 'smart cities'; it is interesting to see how the concept developed. A number of 'definitions' are available for 'smart cities': let us look at some of them here. According to the definition quoted by Professor Mark Deakin, Edinburgh Napier University, (http://www.eib.org/attachments/documents/jessica_smart_cities_deakin_presentation_en.pdf) '*A Smart City is a well performing city built on the "smart" combination of endowments and activities of self-decisive, independent and aware citizens.*' Note that in this definition, the words 'independent' and 'aware citizens' are important. One of the characteristics of smart cities is that they use digital services as the foundation to support the development of 'green' technologies (see Box 10.6) and to support the 'smart' utilization of basic services such as water, electricity, gas and for 'smart transportation' by utilizing these 'smart utilities' as the basic facilities in the built environment of the 'smart infrastructure' of the cities. Most smart cities in the world use as much as possible the solar energy as well as energy from other source of renewable energy (hydral energy, electricity generated by windmills, etc.) – see Figure 10.17; it shows the smart grid concept explained earlier.

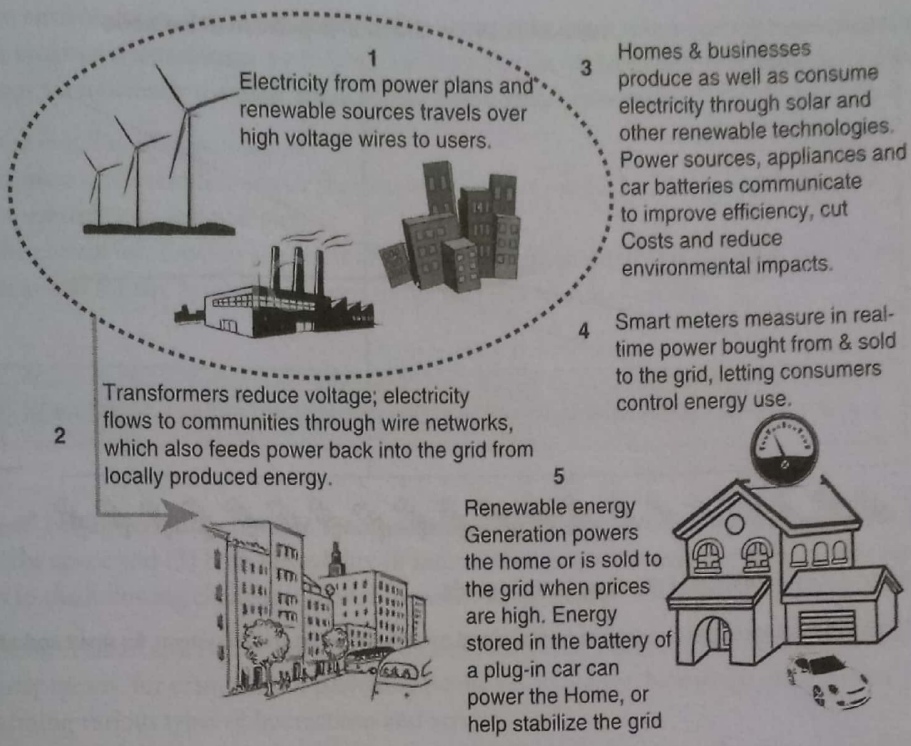


FIGURE 10.17 | The basic concept of a 'smart grid'.

According to yet another definition for smart city, a smart city (sometimes called *smarter city*) makes use of *digital technologies* or ICT to enhance quality and performance of urban services, to reduce costs and resource consumption, and to provide services to its citizens actively and with greater efficiency and more effectively. Another way of defining a 'smart city' is looking upon it as a developed urban area that is based on sustainable economic development and is capable of providing a high quality of life by excelling in multiple key areas, for example, economy, mobility, environment, people, and government. Excellence in key areas mentioned can be achieved through an efficient and effective use of strong human capital, socio-capital and/or ICT infrastructure.

BOX 10.6

Green Technologies

Smart cities use 'Green Technologies' – a continuously evolving group of methods and materials used for techniques of generating energy in a way that causes minimum damage to the environment. The goals of green technologies are: sustainability, innovation, source reduction, green building and green chemistry, among others with the aim of having no negative impact on the environment. Sustainability means meeting the needs of the societal communities on a continuous basis without damaging or depleting natural resources; in other words, creating a society that in the future can fulfill its own needs. In this context, source reduction means reducing waste and pollution by suitably adapting the methods of production and consumption. Innovation in the context of 'green' means developing alternative technologies that have demonstrated lesser damage to our health. The energy crisis is our most critical issue and green technologies recognize this issue of great concern. Green buildings are also part of 'green thinking'.

The origin of smarter cities is interesting; the concept originated in the face of world's worst economic crisis. IBM has been one of the pioneers in this domain. IBM began work on a 'smarter cities' concept in 2008; it was as part of its Smarter Planet initiative. By the year 2009, the concept captured the attention and imagination of several countries started taking part in smart cities initiative. The high rate of urbanization (see Figure 10.18) and the strain on rural land made governments

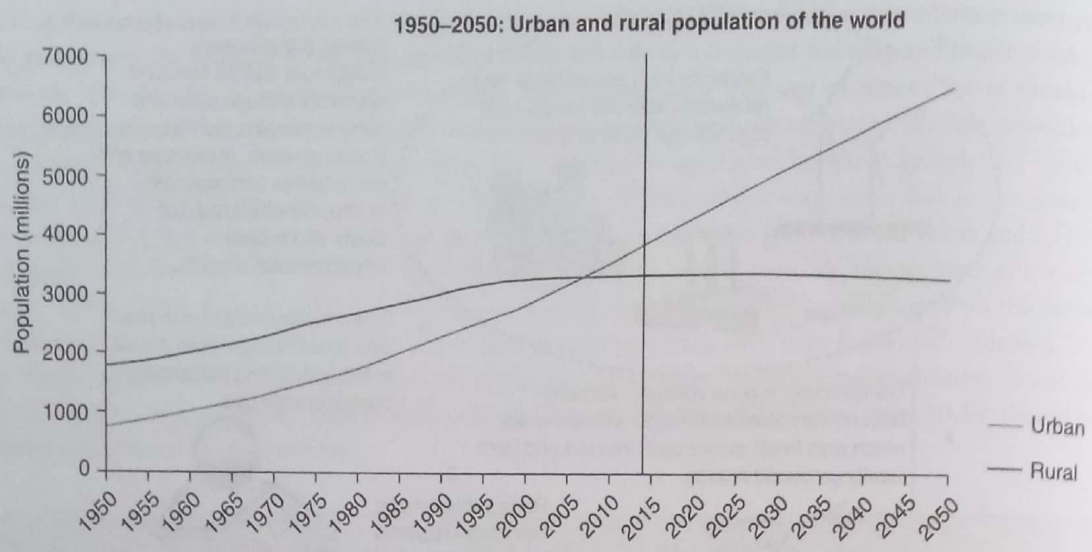


FIGURE 10.18 | Urban and rural population of the word in the decade.

Source: Alessandro Zanni, a computer engineer and an expert in pervasive and context-aware distributed systems, for smart and adaptive environments, 20 April 2015.

across the world realize the need for designing cities capable of coping with the challenges of urban living – subsequently, the announcement of '100 smart cities' fell in line with this vision. As explained before, 'smart city' is an urban region characterized by high level of advancement in terms of its overall infrastructure, sustainable buildings, communications and green markets that have a 'green supply chain'. A smart city embraces ICT as the principal infrastructure and the basis for providing fundamental and necessary services to those who live in it. There are multi-technology platforms involved such as sensor networks with a high degree of automation and green data centers. Even if at this moment all this may sound futuristic or like a Sci-Fi, it is now likely to soon become a reality as the 'smart cities' movement unfolds even in a developing country India. Smart cities do face a number of challenges; of those, privacy and security challenges are what we discuss in this section. Remember that IoT connected devices abound in smart cities. That should point us the flavor of the challenges in security and privacy area for smarter cities.

BOX 10.7

People in the Cities of the World and the 'Triple Play'

It is said that for the first time in history, in 2007, the majority of the world's population (3.3 billion people) lived in cities. It is estimated that by 2050, the number of people living in cities will constitute 70% of the Earth's total population, that is, 6.4 billion people. These billions of people are 'information hungry' – while we wonder whether each one of them indeed has a genuine reason 'hunting' for so much information! Data, information, knowledge and wisdom – though all are parts of 'intelligence' – each dwells at a different level.

In the recent times, there has been a convergence of all types of data – this is often referred to as the 'triple play', that is, the convergence of all types of data as mentioned (i.e., video, voice and text) into our homes and offices – often all coming from a single vendor, and all types of data streamed to a variety of consumer devices (television sets, smart phones, computers, to name a few) 'triple data' is the reality in today's modern world!

'Smart spaces', for example, smart homes, smart buildings and smart cities that are based on IoT connected devices and systems have security challenges that originate from and are related to the philosophy of smart environments; the philosophical concept of smart environment lies in providing freedom to people to use available devices for the purpose of 'information anywhere and at the tip of finger', that is, seamlessly, effortlessly without human-intervention placing in the hand of end-users all the information that they may need. However, given that information security is one of the critical issues of the software-intensive systems, it needs very special solutions for balancing user-friendliness *vis-a-vis* trustworthiness of those systems that

are to work in smart environments. Let us understand why a smart place or a smart environment creates security and privacy challenges. We can envisage a smart space to be a logical entity of an environment that provides information about users' physical surroundings via inherently dynamic applications. Smart spaces have goals:

1. To increase the visibility of opportunities.
2. To support context understanding (recall the discussion in Section 29.5 of Chapter 29 about privacy considerations in the use of context-sensitive technologies).
3. To provide the correct information at a point of time and at a place where it is required, even if not explicitly requested, with its content and format optimally adapted to the user situation and profile.

To revise the fundamentals of information security: you may like to revisit Chapter 4.

The very purpose' behind creating a 'smart space' defines security requirements for: (1) what information is provided, (2) who could use the space and (3) how the validity of information is guaranteed. The free use of information provided by smartspaces results in the following challenges related to information security:

1. **Authentication:** A smart space must provide the facilities for a user, his/her device and application to authenticate with various security means, for example, ID, password, public key exchange, biometrics (see Chapter 11), etc. It is required before performing various types of interactions and actions.
2. **Access control and authorization:** A smart space must control the accesses of appliances and related authorizations (the concept was touched upon in Section 10.4 – Intelligent Buildings). Thus, when a user or application attempts to access to a smart space, the space should check to verify if indeed the requester has access to information or an appliance in question, that is, whether he/she is 'authorized'. This also regards any software update, which should not violate the rules for access control.
3. **Privacy preservation:** A smart space is to assure integrity and privacy of (shared) information: (1) information about the entities connected to the smart space must be protected when it is being transmitted from an information provider to an information consumer (recall 'man-in-the-middle attack' explained in Section 9.5 of Chapter 9), (2) the space should provide solutions that prevent unauthorized corruption of transmitted information and (3) privacy is the basic hygiene in a smart environment/smart space, that is, privacy is the *must*; information related to persons and their preferences/behaviors in the smart space is to be secured (refer to Section 27.9 of Chapter 27 to IPPs to touch base with information privacy principles).
4. **Non-repudiation:** A smart space might have to support non-repudiation of performed operations on applications and requests made by application users. Thus, all actions performed by a user or an application must be logged and associated to the source of the action. Refer to Figure 10.9 – in this context, for example, the action performed by a building maintenance staff has to be associated to the person who completed the task.
5. **Protection from malware:** Users in smart spaces as well as smart places ought to be protected from virus infections and the effects of other malware. In addition, use and forwarding of unsafe content to users and applications are also to be prevented.
6. **Security auditing mechanism:** A smart space should support the means of (real-time) auditing and must also allow preserving security levels of applications and the smart space itself.

Remember...

The security and privacy challenges mentioned above are based on the requirements derived from a large set of application scenarios in which the author was involved to lead a team of application analysts in the project. The team identified and defined those requirements for smart personal spaces smart indoor spaces that were part of smart cities. Note that, even if all the requirements mentioned may not be part of the design for all kinds of smart spaces, they all nevertheless are the architectural requirements of high importance.

As the physical worlds are merging with cyber worlds, there is an ever growing need to bring in a synergy of both the worlds – cyber and physical worlds. As discussed in Chapter 6, smart devices are becoming greatly sophisticated with their amazing capabilities and yet their costs seem to be dropping every year, thus improving their cost to performance ratio year on year. Several of these smart devices (most of which can be connected in the IoT) need around them high-speed wireless networks, including 4G cellular networks. With IoT, it looks like almost every object can retrieve information from the digital environment and then manage and share that information with other devices or users. As seen in this chapter, the IoT and IoT connected smart devices will continue to play a pivotal role in intelligent buildings and smart cities of the future. Thus, smart cities can be viewed as wide-scale cyber-physical systems wherein sensors can monitor cyber and physical indicators and with actuators dynamically changing the complex urban environment in the way or the other. Safe computing in such cyber-physical systems is of utmost importance; let us discuss that here. Technology industries, governments and organizations are now measuring up to the challenges of increased urbanization, striving to improve urban life by offering improved efficiencies with energy utilizations or services along with cybersecurity for smart cities.

From a futuristic perspective, there are a number of challenges; most of them come from the requirements of cyber-physical systems and smart cities to be successful. Those challenges are not so difficult from a technical perspective, the issue is of getting the people of smartcities to co-operate in a techno-social way. Basically, people need to think and act differently given the 24 × 7 connectivity among people, their devices and businesses. People also need to have a greater involvement in smart city life. Technology today allows for distributed computing and sharing information among users, and building a collective intelligence. One of the keys for the success of cyber-physical systems and smart cities is 'collective intelligence'. Collective intelligence uses the crowd-sensing for the cooperative monitoring of the urban environment. It also targets collaborative achievement of operations to perform tasks of general interest in an efficient way. Some of the challenges are: (1) data management, (2) privacy, (3) security reliability, (4) data heterogeneity, (5) reliability and (6) challenges pertaining to real-time processing – they are summarized in Table 10.1. Figure 10.19 shows the elements related to the (data) privacy challenge of smart cities.

TABLE 10.1 | Smart cities: Identity, anonymity and dimensions of privacy space

#	Challenge type	Implications
1	*Data Management*	We receive 'Big Data' (see Chapter 7) comes from various connected devices. It needs to be stored, analyzed and processed to present real-time results. Data can be managed with a combination of offline or online stream processing depending on the goals of the system. With an online stream, information can change often due to real-time conditions and are based on adaptive and continuous queries.
2	Privacy	See Figure 10.19 and also Chapter 27. Today, data changes hands like never before; due to 24 × 7 connectivity, anytime–anywhere computing. In such paradigm, the challenge is to balance privacy concerns and personal data control, at the same time addressing the needs of people in smart cities to access data. *Cyber-physical spaces* and smart cities need to manage terabytes of data which often includes including sensitive information like protected health information and other personal sensitive data such as gender, religion and many others – due to this, significant issues about data privacy emerge. Therefore, we need privacy policies to be in place in order to address privacy issues, for example, we may need tools to manage data anonymity to have information anonymized, that is, need to be made anonymous (its link with any real person needs to be removed before getting the data processed through the systems in smart cities). Figure 10.19 show some important elements of (data) privacy – refer to Chapter 27.
3	Security	For smart cities also, just like in case of all communications, we must ensure security during communications because all actions among IoT connected devices are synchronized in real time. As smart cities expand they lead to the increase of interactions between physical and cyber systems (thus creating cyber-physical spaces), security problems impact more smart cities.

TABLE 10.1 | (Continued)

#	Challenge type	Implications
		This implies that conventional infrastructures for security no longer would be able to address the issue or may not be sufficient. New solutions must be found for securing information in smart cities. Given the trends in modern business analytics, information security issues become critical for new data coming into smart cities as well as the stored data inside smart cities collected for future use. *Cyber-physical spaces* are based on heterogeneous applications and wireless communications – this may raise critical security issues.
4	Data heterogeneity	The design of communication protocols and the performance of communication across the networks are significantly impacted by data heterogeneity. Systems need to be able to support a large number of applications and devices but also a variety of data such as what we get due to 'Big Data' (refer to Chapter 7).
5	Reliability	In critical contexts such as infrastructure, healthcare, transportation and several others, cyber-physical spaces are appropriate to use. Reliability and safety are basic requirements because of the manner in which sensors and actuators affect the computing environment. Indeed, the impact of sensors and actuators can also be irrevocable, and therefore, the possibility of out of the blue behavior of information systems must be minimized. In addition, the computing environment may not be predictable so *cyber-physical spaces* must continue to work even when there are unforeseen circumstances and must adapt themselves in case of system failures.
6	Real time	As mentioned before, smart cities are cyber-physical spaces and as such, they need to handle large amounts of data that is received from multiple sources given the IoT environment in the modern high-tech area. Therefore, computation mechanisms ought to work efficiently and in a timely manner. This is because physical processes continue independent of computation results. Adequate network bandwidth system capacity needs to be instituted to satisfy this requirement in order to meet time-critical functions of the IT applications under use because failures on the time of actions can cause permanent damages.

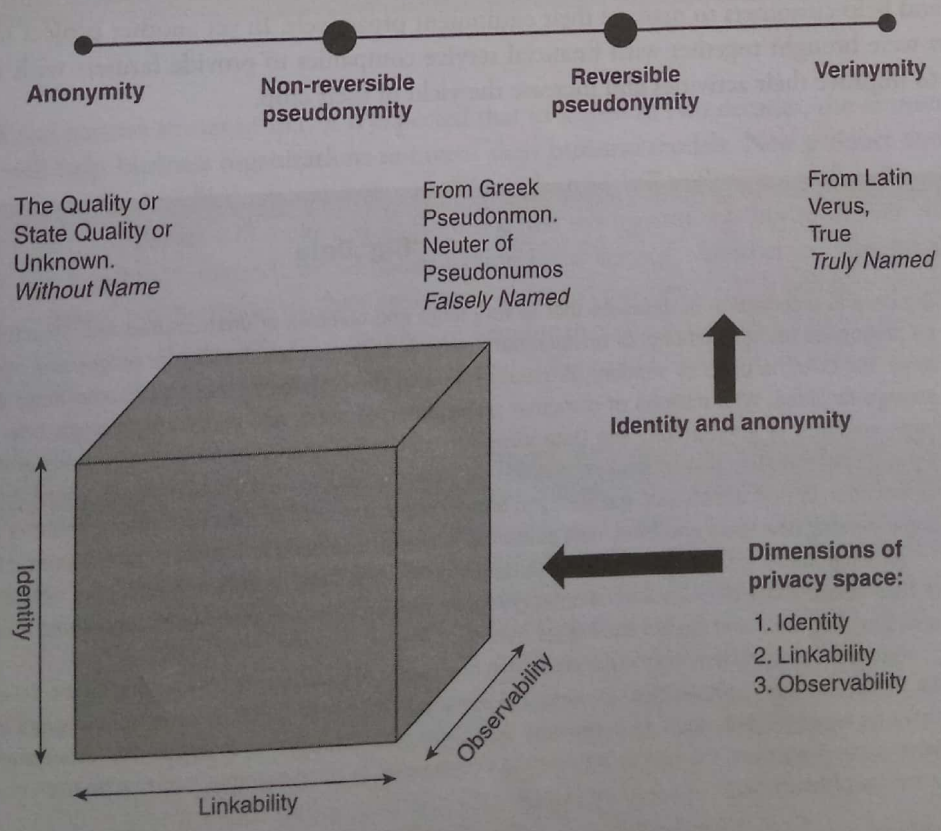


FIGURE 10.19 | Data privacy challenge of smart cities.

10.6 Personal and Business Impact of IoT

It is good to think how the IoT is going to impact us in the future years because the new rule is going to be 'we shall connect anything that can be connected'. Of course, at a philosophical level, the question is why on Earth would we want to be 'so connected' all the time and why should we care to have so many connected devices 'talking' to each other, that is, electronically communicating with one another? As an example of an implication of such scenarios or as an example of the potential value of super connectivity with IoT, consider this: suppose a high position executive or a high position officer is on his way to a meeting, his car could have access to his calendar and already know the best route to follow. During heavy traffic, his car might send a text to the other party notifying them that he is most likely to be late. As another example, imagine that your alarm clock could wake you up you at 6 a.m. and then notifies your coffee maker to start brewing coffee for you. What if your office equipment and what if your refrigerator (with an IP address and therefore capable of being connected on the IoT) knew it was running low on supplies and automatically and therefore the refrigerator would re-order the required food stuff! How about your wearable device that you use in the workplace telling you when and where you were most active and productive and further what if that device shared that information with other devices that you use while working? Chapter 28 helps you to get a flavor of a similar scenario – read the scenario presented in Box 28.17 of Chapter 28. Are these potential scenarios for person privacy invasion? Think about it and then ask yourself about the relative merits and downsides of IoT. To some people, the 'IoT' may mean nothing more than a highly hyped word or a futuristic term. However, IoT is already here and improving our lives. Consumers and businesses are already getting the benefits of multiple machines, devices and appliances connected to the Internet through multiple networks. Both consumers and businesses are getting innovative new services. Our society is poised for moving beyond smartphones, tablets and other consumer electronics. What is more, wireless connectivity is now being added to a variety of machines, including vehicles, household appliances, monitors and sensors and as mentioned earlier the 'wearables', that is, wearable digital devices.

It is said that the Industrial IoT holds the potential to result into a wide range of improvements for businesses. A number of businesses have already reaped the benefits from using the industrial IoT in their business activities. For example, consider the case of a large oil company (the real name concealed for business privacy reason) – at the refineries of this large oil company, employees wear a wireless multi-gas detector. This way, they track their exposure to dangerous gases. Using RFID tags, employees can be monitored (privacy invasion due to this is another issue), or they can press a panic alarm themselves when in danger. Another industrial equipment giant organization (name not disclosed due to business privacy reason) informs its dealers using industrial analytics. Data generated by machines, engines is and transmitted to dealers. This, in turn, allows them to predict problems and help customers to manage their equipment proactively. In yet another project in India, a number of equipment producers were brought together with financial service companies to provide farmers with the information that they need to be able to improve their activities and increase the yield of their crop.

BOX 10.8

'Big' Data

Big Data is a collection of datasets that is very large and complex of unstructured and structured data that cannot be processed using traditional or on-hand database management and traditional processing applications. When the term 'Big Data' is used by vendors, it usually refers to the technology that can handle large amounts of data and storage facilities. With millions of computer users, Internet users and all this technology, how do we manage such large amounts of information? Big Data sizes are constantly changing; from 2012, there were a few terabytes to petabytes of data in a single dataset. Improvements in the traditional database management system (DBMS) and the introduction of new databases, the ability to handle larger amounts of data is in reach. There is still some difficulty in implementing new tools and thus, new platforms is being developed to handle different types of large data.

Although there is no single and precise definition for 'Big Data', a generally accepted definition is this: *'Big Data' is data whose scale, diversity and complexity require new architecture, techniques, algorithms and analytics to manage it and extract value and hidden knowledge from it.*

Gartner (the world famous industry research organization) included big data among its top 10 strategic technologies for 2012. The *size, complexity of formats* and speed of delivery of these *massive datasets* will require new or unique tools for management, such as in-memory DBMS. In addition, Gartner foresees the replacement of the single data warehouse model and the rise of logical data warehouses to bring together information from multiple sources and in a variety of forms.

BOX 10.8 (Continued)

Big Data is not just about its quantity being very large; there are four dimensions of Big Data: (1) Variety, (2) Velocity, (3) Volume and (4) Veracity. The fourth dimension of Big Data is contributed by IBM – much of the 'data growth' consists of semi-structured and unstructured data, such as emails, audio, video, blogs, as well as machine-generated data.

Refer to Figure 10.20; it shows the Big Data 'math', that is, explains the orders of magnitude of Big Data.

Exabyte, Megabyte, Gigabyte, Terabyte

Decimal Value	Symbol	Metric	Binary Value
1000	KB	kilobyte	$1024 = 1024^1 = 2^{10}$
1000^2	MB	megabyte	1024^2
1000^3	GB	gigabyte	1024^3
1000^4	TB	terabyte	1024^4
1000^5	PB	petabyte	1024^5
1000^6	EB	exabyte	1024^6
1000^7	ZB	zettabyte	1024^7
1000^8	YB	yottabyte	1024^8

FIGURE 10.20 | The Big Data bytes.

Given such trends and success stories of IoT, it is expected that in a span of two decades, the economic and employment potential of the IoT will help business organizations re-invent their business models. New product and service hybrids will be developed to help them generate fresh revenue streams. The industrial IoT will promote the rise of the 'outcome-based economy'. This means that companies will make a shift from not just selling products but to deliver 'measurable outcomes'. We will no more pay for a product; instead, we will start paying for a 'service'. Another example of this in the healthcare industry is 'out-come'-oriented payments rather than 'treatment'-oriented payments – this will be a revolution saving millions of lives in case of critical diseases. Thus, there are a number of benefits that the IoT provides to business: these benefits of IoT are summarized in Table 10.2. The increased use of devices globally, due to IoT, is shown in Figure 10.21.

TABLE 10.2 | IoT benefits to businesses

Benefits of IoT	What it means
1. *Productivity boost*	We will soon be in a techno-cultural world, that is, a tech-driven culture. It will no longer be a dream to envisage the idea that we can be monitored by smart technology in exchange for free products, services or some kind of value addition. Humans have the inherent tendency to seek rewards. The concept of 'gamification' is based on this human desire – it is essentially the application of game elements in real-life situations.
2. *Generation of new revenue streams*	IoT is beginning to change the business landscape. There will be an increasing demand for newer products and services that are harmonious with the changes. Businesses will see new opportunities to develop these products and services, thus generating revenue streams that did not exist previously. There is no doubt that many businesses will surface and many others will undergo diversification as a result.

TABLE 10.2 (Continued)

Benefits of IoT	What it means
3. *Creating better customer experience*	As 'intelligent devices' 'talk' to each other, we move toward an era of hyper-connectedness or what we can also call 'connected living' – that way customers will be empowered like never before, connected 24 ×7, and much more well-informed than they already are.
4. *Improved business intelligence*	Big data is Big! See Box 10.8. Managing Big Data and mining meaningful information out of it has been one of the most challenging tasks for businesses; we are now just beyond management information system. We need much more sophisticated decision support systems for our business analytics. IoT could make it easier to collect more relevant information from the depths of the Internet. With IoT working for us, there will be data rushing in from all sources that we can think about for the data – hospitals, offices, homes, shopping centers, gas stations and every other imaginable spaces – remember the discussion about 'smart cities' and about sensors and actuators (Box 10.1). All of that data will present a massive opportunity for businesses.

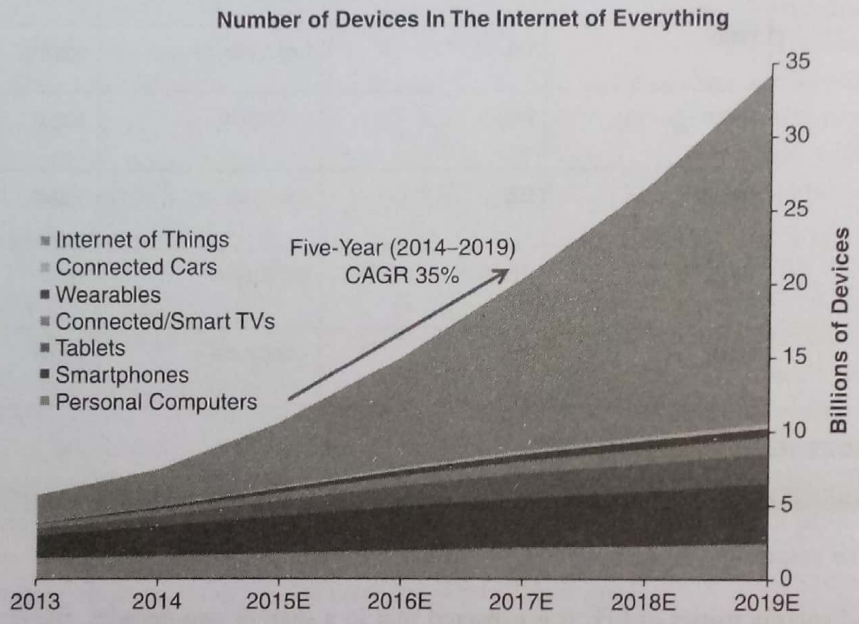


FIGURE 10.21 | Devices in use globally due to the IoT.

SUMMARY

In this chapter, we learned about the IoT and its impact in our life in the future years. We learned how the IoT works and how it has provided opportunities for 'wearable computing'. We discussed about 'intelligent buildings' and 'smart spaces' – one example of whose is 'smart cities'. The concept of 'smart planet' is also introduced in this chapter. We also learned about the security and privacy implications in these scenarios. Intelligent buildings represent a classic application of systems integration. In the face of global energy crisis, we need for new energy efficient interventions, we also need real-time decision support given the speed and complexity of global businesses. To be offered an easy access to key performance indicators, we need enhanced building and personnel security and better dashboards for managing complex information. In a way, all these are the drivers for intelligent buildings. However, security and privacy risks do arise from the integration of systems that traditionally had been stand-alone.

The world is here to embrace the technological evolution that the IoT, cyber-physical spaces, wearable computing and the entire gamut to bring revolutions to our everyday lives. The expectation is that these technologies will enhance the quality of services and will ultimately provide environmental benefit as they will get implemented or are already being implemented in smart cities (mainly in developed countries) throughout the world. The concept of cyber-physical spaces will continue to be a driver of innovation; it involves multiple disciplines and multiple technologies. Industries too will start getting influenced by the concept of cyber-physical spaces and many

applications of the concept will get developed for industry use. However, such technological innovations, when put to practical use in our day-to-day life, cannot work effectively without a highly skilled workforce. Moreover, we also need fruitful collaborations between industries and universities. Finally, the IoT and all its related applications have the huge potential to impact, change and improve every aspect of our lives, addressing critical challenges for our society. Soon, they could exceed today's distributed systems from the perspective of security; performance orientation, efficiency, reliability, usability and many other related aspects. A final thought – our life is going to be nothing but 'connected living'!

Review Questions

1. What is 'the IoT'? Explain briefly how it works.
2. What are the underlying protocols to make IoT work?
3. What is an 'intelligent building'?
4. What do we mean by 'wearables'?
5. Explain the concept of 'smart planet'.
6. Highlight the physical security aspects of intelligent buildings that you believe as very important.
7. What are the drivers that have led to 'intelligent buildings'?
8. Is cyber security important for intelligent buildings? Explain how.
9. Highlight the privacy and security issues in smart cities.
10. Describe with examples, in what way the IoT will impact our personal lives and businesses.

Further Reading

A number of video clips on IoTcan be watched by visiting the list of URLs quoted below (all accessed on 25th July 2015).

The Internet of Things (IBM Social Media): https://www.youtube.com/watch?v=sfEbMV295Kk

Intel IoT– What Does The Internet of Things Mean?: https://www.youtube.com/watch?v=Q3ur8wzzhBU

The Internet of Things: Dr. John Barrett at TEDxCIT: https://www.youtube.com/watch?v=QaTIt1C5R-M

Introduction to the Internet of Things: https://www.youtube.com/watch?v=RCIyogqzI6c

Windows and the Internet of Things: https://www.youtube.com/watch?v=UVmSNAD9ivc

What is The Internet of Things?: https://www.youtube.com/watch?v=wL34vK-On3o,https://www.youtube.com/watch?v=wL34vK-On3o

How Intel Technology Enables IoT: https://www.youtube.com/watch?v=ROadFidEDgM

Transform Manufacturing with the Internet of Things: https://www.youtube.com/watch?v=5OQQZ9eWF-4

What Is the Internet of Things?: https://www.youtube.com/watch?v=TkV1JMvtivA

The Internet of Things: http://www.fwthinking.com/video/clips/fwthinking-ep1-internet-of-things-video/

Internet of Things as Fast as Possible: https://www.youtube.com/watch?v=BQzBpUdHvi4

The Internet of Things (and With Things) – read the article at this URL (accessed on 21st July 2015): http://www.comsoc.org/blog/internet-things-and-things

A small video about the Internet of Things (IoT) can be watchedat this URL (visited on 21st July 2015): http://shows.howstuffworks.com/fwthinking-show/fwthinking-ep1-internet-of-things-video.htm

In the context of the working IoT–the URLs quoted below have the reading that would help you understand about client–server architecture:

http://www.webopedia.com/TERM/C/client_server_architecture.html

https://en.wikipedia.org/wiki/Client%E2%80%93server_model

In the context of the working IoT, it would be of interest to visit the link mentioned below (accessed 22nd July 2014) to understand Message Formatting: Headers, Payloads and Footers: http://www.tcpipguide.com/free/t_MessageFormattingHeadersPayloadsandFooters.htm

In this chapter, a number of scenarios relating to the 'digital future' have been mentioned. Perhaps, as a culmination of those scenarios, readers may be interested in seeing the movie 'HER'. The movie shows us the growing capabilities in artificial intelligence and self-evolving the operating system so 'smart' that the protagonist develops a personal relationship with his operating system that he has installed with the option of the OS to speak to him in a female voice. Spike Jonze in 2013 wrote, directed and produced the movie Her. The movie is an American romantic science fiction comedy-drama film. For further information, visit the URL mentioned below (accessed on 23rd June 2015): https://en.wikipedia.org/wiki/Her_(film).

For a video clip about 'An Introduction to IBM's Smarter Planet', you may like to visit the URLs quoted below (accessed on 21st July 2015): https://www.youtube.com/watch?v=QZ0o7avcvv4

In reference to [1], number of transistors per person, mentioned in Box 10.1 you can visit the URL: https://www.voltage.com/technology/over-1-billion-transistors-per-person/ accessed on 20th July 2015.