K.S.Rangasamy College of Arts & Science

(Autonomous)

Ksr Kalvi Nagar,Tiruchengode-637215.Namakkal Dist.

Tamil Nadu,INDIA.

iHORE

Issue #93

May 2016

Department Of Computer Science and Computer Applications

Ishare

Editorial

We would like to wholeheartedly thank our honorable Chairman, Secretary, Executive Director and Principal for their continuous encouragement and constant support for bringing out the magazine. We profoundly thank our Head of the Department for encouraging and motivating us to lead the magazine a successful one right from the beginning. Ishare serves as a platform for updating and enhancing upcoming technologies in Information and Communication. We are grateful to all the contributors to this magazine so far. The magazine has been sent to almost 60 Institutions in and around Tamilnadu. So far we have received feedbacks and appreciations from various Institutions.

We would be very pleased to receive your feedbacks. Please send your feedbacks to ishare@ksrcas.edu

By,

Editorial Board

CONTENTS

1. FIVE GROWING IT INDUSTRY TRENDS & DEVELOPMENTS

Ms. A.Nirmaladevi, Ms. S.Latha & Ms. S.Gowri
Asst. Professors in CS

List of 5 top industry trends changing the face of IT to help our business prepare for the fast-approaching future:

1. **Mobile Devices** --The basic tools that businesses and consumers use to interact with each other are currently undergoing a major behavioral shift. More than one-third of the conventional PC market is on the verge of being replaced by smartphones and tablet computers in the coming year and this trend shows no signs of slowing. By 2014, it is predicted that mobile Internet usage will overtake traditional desktop usage.

2. **Cloud Computing** --As businesses look for new ways to scale back on overhead and infrastructure costs, they are turning increasingly to Software-as-a-Service (SaaS) and other cloud-based computing solutions. Spurred in no small part by growing consumer confidence in this new technology, more and more businesses are discovering the advantages of moving their software applications to remote private cloud

networks. As the economy recovers and growth resumes, these solutions allow for low-cost, on-demand scalability.

3. Virtualization --Just as cloud computing and SaaS have revolutionized the way companies access their software applications, recent trends in virtualization are allowing businesses to eliminate entire server farms and slash the associated operating costs. In addition to streamlining and making IT infrastructure more economical and flexible, server virtualization has laid the groundwork for more strategic IT initiatives going forward. As a result, Infrastructure-as-a-Service and Platform-as-a-Service (IaaS with a software development framework) are also growing in popularity.

4. Telework / Virtual Offices --With cloud computing capabilities and other advances in office connectivity growing by leaps and bounds, companies worldwide are realizing the cost-saving benefits of virtual office environments. By moving away from traditional physical office-based business models toward remote network structures, more and more businesses are taking advantage of this new technology to increase productivity and reduce overhead.

5. Alternative Productivity Applications -- Influenced by the recent economic downturn, companies are looking for new methods of improving productivity, increasing employee efficiency and optimizing their overall business processes. In this pursuit, new solutions in videoconferencing, unified communications and business intelligence

applications will continue to grow and develop, since they help employees to work collaboratively in remote office environments. In addition to improvements in these already established areas, there is considerable demand and room for growth in the productivity software sector, with more and more businesses adopting new programs designed to improve efficiency, lower operating costs and streamline business processes.

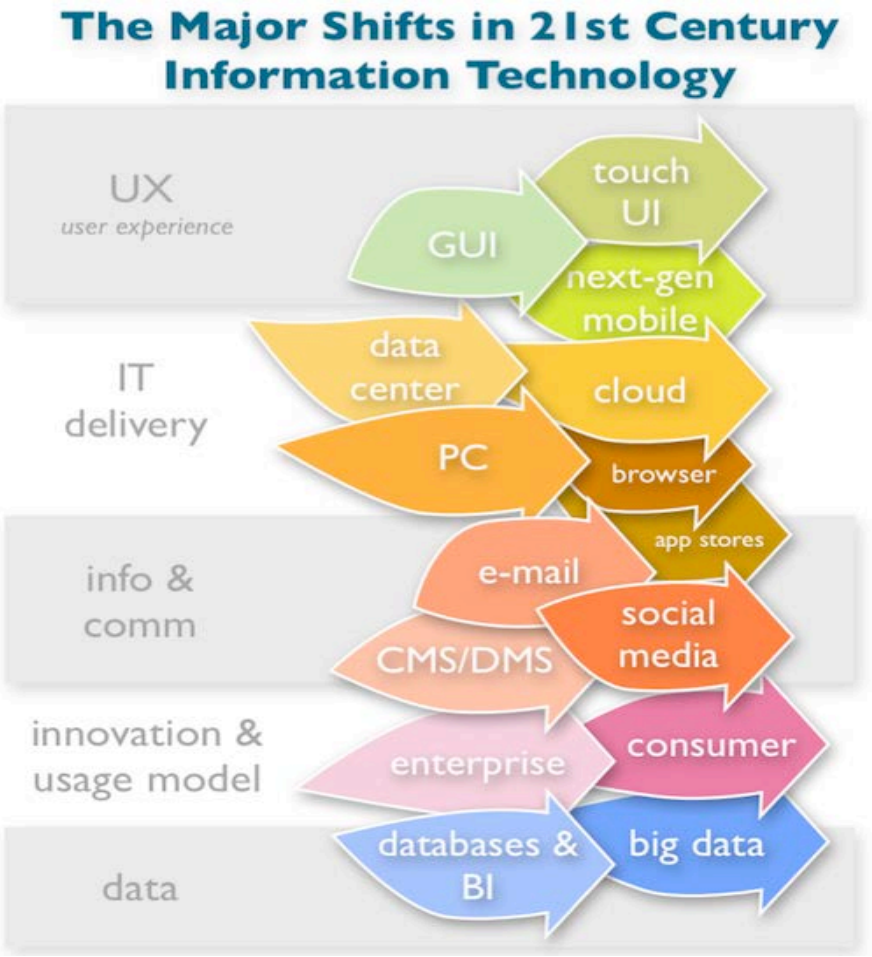
2. THE "BIG FIVE" IT TRENDS OF NEXT DECADE

R. Nirmala, Assistant Professor

The "Big Five" **IT trends of the next half decade: Mobile, Social, Cloud, Consumerization**, and **Big Data.**

1) Next-Gen Mobile - Smart Devices and Tablets

Smart mobile devices based on iOS, Android, and even Blackberry OS/QNX are seeing widespread use. But comparing projected worldwide sales of tablets and PCs tells an even more dramatic story. Using the latest sales projections from Gartner on tablets and current PC shipment estimates from IDC, user can see that by 2015 the tablet market will be 479 million units and the PC market will be only just ahead at 535 million units. This means tablets alone are going to have effective parity with PCs in just 3 years.



Challenges to smart device adoption:

- **Smart devices have a poor enterprise ecosystem today:** Enterprise software vendors and IT departments have organized around older platforms such as Windows and LAMP. Their infrastructure, skills, and relationships are largely built around an older generation of IT. In the meantime, iOS and Android have a lot to learn and to build up

to begin to match this world, though they are starting to make progress in this regard.

- **Many of the inherent advantages of smart mobile are anathema to structured IT:** From app stores to HTML 5, the large and easy to access application universes of next-gen mobile immediately triggers a security lockdown response (right reaction, wrong response) from IT. IT departments desire to remove app stores from smart mobile devices entirely. The solution is probably policy-based screening of apps.

2) Social Media - Social Business and Enterprise 2.0

Mobile phones technically have a broader reach than any communications device, social media has already surpassed that workhorse of the modern enterprise, e-mail. Increasingly, the world is using social networks and other social media-based services to stay in touch, communicate, and collaborate. Now key aspects of the CRM process are being overhauled to reflect a fundamentally social world and expecting to see stellar growth in the next year. As Salesforce's Marc Benioff was very clear in his dramatic keynote at Dreamforce last month, leading organizations are becoming social enterprises.

Challenges to social media adoption:

- **Social media is not an IT competency.** Simply put, the human interaction portion of social computing is generally not IT's strong suit. It tends to be treated as just another application to roll out instead of being integrated meaningfully into the flow of work.
- **The more significant value propositions of social require business transformation.** Maintaining a Facebook page and Twitter account is relatively straightforward and necessary, but it usually won't generate significant growth, revenue, or profits by itself either. The more profound and higher order aspects of social media including peer production of product development, customer care, and marketing require deeper rethinking of business processes.

3) Cloud computing

Cloud computing is one of the more interesting and controversial. While there are far more reasons to adopt cloud technologies than just cost reduction, according to Mike Vizard perceptions of performance issues and lack of visibility into the stack remain one of the top issues for large enterprises. Cloud computing is being adopted steadily for non-mission critical applications and some are now even beginning to downsize their data centers. Business agility, vendor choice, and access to next-generation architectures are all benefits of employing the latest cloud computing architectures, which are often radically advanced compared to their traditional enterprise brethren.

Challenges to cloud computing adoption:

- **Concerns of control.** When jobs depend on IT being up and working, then user can be sure there will be reluctance to adopt the cloud.
- **Reliability and performance perceptions.** Widespread outage by Amazon and Microsoft in the past has set back cloud adoption a minor amount, yet uptime is still extraordinary good by most enterprise standards. More of an issue is moving the enormous datasets that enterprises now possess into and out of the cloud quickly enough. Backhaul and other methods will need to improve substantially to address this satisfactorily for large enterprises.

4) <u>Consumerization of IT</u>

Consumerization also very much has to do with its usage model, which eschews enterprise complexity for extreme usability and radically low barriers to participation. Enterprises which don't steadily consume their application portfolios are in for even lower levels of adoption and usage than they already have as workers continue to route around them for easier and more productive solutions. Another decentralized and scalable solution is, as with next-gen mobile, to help workers help themselves to third party apps that are deemed safe and secure.

Challenges to applying consumerization to IT:

- **Vendors provide the UX.** Usability and low barriers to participation won't exist until third party vendors, which provide a large percentage of IT, get the message and overhaul their apps.
- **Consumer technology often isn't enterprise ready.** At one point, neither was open source, but eventually an industry that provided value-added services emerged. The same pattern is likely to happen with popular consumer apps.

5) Big Data

The term "Big Data" was coined to describe new technologies and techniques that can handle an order of magnitude or two more data than enterprises are today, something existing RDBMS technology can't do it in a scalable manner or cost-effectively.

Big data offers the promise of better ROI on valuable enterprise datasets while being able to tackle entirely new business problems that were previously impossible to solve with existing techniques. While most companies are still addressing their big data needs with data warehousing.

Challenges to adopting Big Data:

- **Big data requires many new skills.** There are a host of advanced technologies and new platforms to learn to be effective with

big data, and the IT departments are concerned about the skills they must acquire or foster internally to take advantage of them.

- **Meaningful use of big data requires considerable cross-functional buy-in.** Big data requires tapping into silos, warehouses, and external systems using new techniques. SOA has similar challenges because it had to coordinate and align so many parts of the business. While some big data will be single function, many of the more intriguing possibilities requires a lot of cooperation across the business and with external vendors, not at easy task.

3. TOP TEN COMPUTER TRENDS FOR 21st CENTURY

B. Sowmya, Assistant Professor
Department of Computer Application

1. Computers will become powerful extensions of human beings designed to augment intelligence, learning, communications, and productivity.

2. Computers will become intuitive—they will "learn," "recognize," and "know" what we want, who we are, and even what we desire.

3. Computer chips will be everywhere, and they will become invisible-embedded in everything from brains and hearts, to clothes and toys.

4. Computers will manage essential global systems, such as transportation and food production, better than humans will.

5. Online computer resources will enable us to download applications on-demand via wireless access anywhere and anytime.

6. Will become voice-activated, networked, video-enabled, and connected together over the Net, linked with each other and humans.

7. Computers will have digital senses-speech, sight, smell, hearing-enabling them to communicate with humans and other machines.

8. Neural networks and other forms of Artificial Intelligence will make computers both as smart as humans, and smarter for certain jobs.

9. Human and computer evolution will converge. Synthetic intelligence will greatly enhance the next generations of humans.

10. As computers surpass humans in intelligence, a new digital species and a new culture will evolve that is parallel to users.

4. iTWIN

Ms. A. Anitha Malar
Asst. Professor in BCA

What is an iTwin?

iTwin is a revolutionary new file sharing and remote access device brought to you by a company called iTwin. It's like two ends of a cable, without the cable. It's as simple to use as a flash drive. It’s literally plug and play.

iTwin can connect any two online computers anywhere in the world. iTwin enables you to have access to any or all of your home computer's files and folders while you're on-the-go. Similarly, you can also use iTwin to access to any or all of your office computer's files and folders while on-the-go. There's no in-built limit to the amount of storage you can access with iTwin while you're on-the-go. The only limit is the size of your hard drives. The only other "limit" is the speed of your Internet connection. The faster it is, the better your experience.

You can select files for accessing later on-the-go, or you can edit them remotely, without the files leaving your computer. You can also back-up files to your home or office computer while you're out on-the-go. It's so easy, it's unbelievable.

Who invented iTwin?

iTwin was invented by an Indian named Lux Anantharaman. After achieving a Bachelor's degree in Electrical and Electronic Engineering from IIT in Chennai and a Master's degree from IISc in Bangalore, Lux worked first as an IT Security Researcher at the Institute of Systems Science, Singapore and then as Senior Researcher at Kent Ridge Digital Labs and the Institute for Infocomm Research. Lux specializes in PKI implementations, efficient digital certificate revocations and usable security. Lux was pursuing a part-time MBA at NUS Business School, Singapore, but put studies on hold because of potential of iTwin.

How to use iTwin?

When you connect iTwin, you'll see a regular window pop-up, just as you would if you plugged in a regular USB flash drive. Drag and drop files and folders into this window to share them - as many as you want. Leave your computer with one half of iTwin connected to it. Detach the other half of iTwin and take it with you.

Wherever you go, you can remotely access the shared files, simply by plugging the half you are carrying into any online Windows computer, anywhere. iTwin allows you to transfer files to - or from - your home computer or your office computer or your friend's, or your colleague's! iTwin also allows you to edit the shared files on a remote computer, while keeping them on that remote computer.

FEATURES

1. **Like a Limitless Capacity Secure USB Drive**

iTwin allows you to securely access your entire hard drive. It's as if you are carrying an access-key to all your files in a device that fits in the palm of your hand. And unlike portable storage, iTwin lets your data stay safely at home (or in the office).

2. **Remotely edit shared files**

Remotely edit any shared file from any location. iTwin allows you to keep a single version on one computer, with you and your chosen iTwin partner collaborating directly on this version. Say goodbye to multiple versions of files flying around by email.

3. **Backup your data from anywhere**

When you are on the road, you can use iTwin to move copies of files from your laptop to your home or office computer. If you are traveling and taking lots of pictures, you can free up your SD card by moving files onto your laptop and transferring them back home. It keeps your data safe and secure.

4. **One-time cost. No fees, ever**

Don't pay for cloud storage. Don't pay subscription fees for file access. Don't get locked in. You have all the storage you need on your

computer and home hard drive. With iTwin, share it and access it from anywhere.

5. **Data Security**

iTwin doesn't store any data on itself. It just enables a secure connection between two computers. Your remote data can only be accessed if you have the physical iTwin with you. Additionally, you can set up your iTwin to require a password. iTwin includes a feature that allows you to remotely disable the connection should you lose your remote iTwin half. So you can rest assured that your data is safe, even if you lose your iTwin device. If you have ever lost a portable memory device, you know that terrible feeling. We want to make sure this never happens to you again. It even makes use of AES(256 bit key encryption) in order to transfer the data from one computer to another.

UNIQUE FEATURES

- Smart key generation
- No “Temp Files”
- Password support
- Bi-Directional File Access

- iTwin is like the two ends of a cable, without the cable.

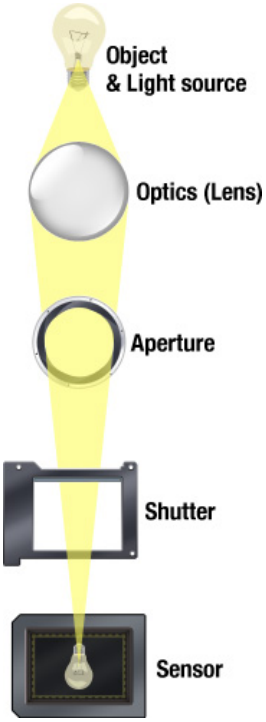
iTwin device has two identical halves. The two halves can be connected together via their special connector to form a pair.

1. **USB Connector**

The USB connector is used to plug the device into the USB port of a computer.

2. **iTwin Connector**

The iTwin Connector is used to connect the two halves of the iTwin device to form a physical pair. It is used to securely transfer a cryptographic key between the two halves of the device during device pairing.



3. **Activity Indicator (LED)**

This indicates the state of the iTwin device. **No Light**: Device is not functional or iTwin is not installed on your computer. **Red Light**: Error Constant. **Blue Light**: Device is active and functioning.

This article is meant to only cover the basics of photography. The idea with this series is to get people more interested in photography,

awaken creativity and hopefully help people enjoy this hobby even more.

5. BASICS OF PHOTOGRAPHY

T. Sridhar
III B.Sc CS "D"

An introduction to Photography

The word "*photography*" is French but is based on Greek word and literarily means "*drawing with light*". That's what photography is all about, without light — no photograph. The art of photography is basically seeing and balancing the light.

The illustration to the left shows the path the light travels from the object to the sensor (or film in non-digital cameras).

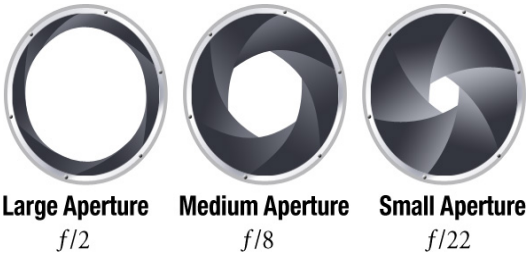
First the light needs to go through the **lens**, which is a series of differently shaped pieces of glass. If the focus is good then the light will meet on the sensor.

The **aperture** is placed inside the lens and is basically an opening that controls how much light reaches the sensor.

On most modern cameras the **shutter** is placed inside the camera body. This piece of mechanics is what controls how long time the sensor is exposed to the light.

The **sensor** is a very sensitive plate where the light is absorbed and transformed into pixels. As you can see on this illustration, the image the sensor picks up is actually upside down, just like our eyes sees the world, the processor inside the camera then flips it.

Aperture



The aperture sits inside the lens and controls **how much light** passes through the lens and onto the sensor.

A large aperture lets through very much light and vice versa. Knowing how the aperture affects the photograph is one of the most important parts of photography — it affects the **amount of light, depth of field, lens speed, sharpness and vignette** among other things.

f-numbers, a mathematical number that expresses the diameter of the aperture, are an important part of understanding how the aperture and **exposure** work. All f-numbers have a common notation, such as ƒ/5.6 for an f-number of 5.6. There are a set numbers of f-numbers that are used in photography, there are several different scales but the "standard" full-stop f-number scale is this:

ƒ/# 1.4 2 2.8 4 5.6 8 11 16 22 32

These are known as **full-stop f-numbers**. If you decrease the f-number with one full-stop, like **ƒ/4** to **ƒ/2.8**, the amount of light that

passes through will double. If you increase the f-number with one full-stop, like **ƒ/5.6** to **ƒ/8**, only half the amount of light will reach the sensor.

There can be several f-numbers between the ones above — depending on what scale is being used. The most common one is a **1/3** scale, which means that every third step is a full-stop, and thus giving you two settings between every full-stop. For example between **ƒ/8** and **ƒ/11** you will find **ƒ/9** and **ƒ/10**. This can be rather confusing at first, so here's a short reminder:

A higher f-number = a smaller aperture = less light

A lower f-number = a larger aperture = more light

Shutter

Open focal-plane shutter Closed focal-plane shutter

The shutter is what controls **how long the sensor is exposed** to the light. The longer the shutter is open; more light can be captured by the sensor. A fast shutter speed will result in "**freezing**" a moving object and a slow shutter speed will let you capture the **motion** of a moving object. There is a scale of stops for the shutter speeds just like for the aperture, below are the full-stops.

1/1000 s 1/500 s 1/250 s 1/125 s 1/60 s 1/30 s 1/15 s 1/8 s 1/4 s 1/2 s 1 s

And just as with the aperture, the shutter speed is often on a **1/3** scale, giving your two steps in between every full-stop. For example between **1/60s** and **1/125s** you will find **1/80s** and **1/100s**.

The two primary factors which control exposure are shutter speed and aperture.

ISO

The ISO speed (the name comes from the *International Organization for Standardization*) is a measure of the **film speed**, or its **sensitivity to light**. With digital cameras, the ISO affects the sensor instead of the film, but the principal is the same. A **low ISO** speed requires a longer exposure and is referred to as slow; a **high ISO** speed requires less time to give the same exposure and is therefore referred to as fast. One step in the ISO equals one full-stop, so the ISO is not on a 1/3 scale — film can be found with 1/3 ISO speeds, but it's uncommon in the digital world. These are the most common ISO speeds.

ISO 50 100 200 400 800 1600 3200

On 35mm film, a film with high ISO speed had much more grain than a slower film — but the modern sensors don't create the same grain with high ISO speeds. Instead it creates **noise**. The digital noise is not as favorable as the film grain and can destroy a photo if it's too visible (the same goes with the grain, but its effect was more subtle and often more liked).

If light is no problem, then always use a low ISO number but if you're indoors with bad light or other conditions when you find the combination of aperture/shutter not to be enough the ISO speed can be a great asset. New digital sensors are constantly developed and the noise levels with high ISO speeds are decreasing with every new release.

6. EIGHT TECH TRENDS TO WATCH IN 2016

R. Sudha, Assistant Professor
Department of Computer Applications

1. **Algorithmic personality detection:**

Did you know that some life insurance underwriters are attempting to assess your personality — via your magazine and website subscriptions, the photos you post to social media, and more — in order to determine how risky an investment you are? Some lenders have used personality algorithms to predict your future financial transactions. Algorithms will harness personal data in order to assess an employee's predicted success at work: for example, how likely she is to bounce around jobs.

2. **Bots:**

Software applications that run automated tasks are called "bots." 2016 will bring a host of creative bots that will supercharge our productivity, keep us company, and help us track what others are doing.

What's new: you'll have the opportunity to use and program them yourself.

Bots do more than offer conversation. News organizations will soon use bots to sort and tag articles in real time. We'll see advanced bots manipulating social media and stocks simultaneously. The intelligence community might deploy bots for surveillance and for digital diplomacy. HR managers can use bots to train employees. Meantime, as Slack continues to grow in scale and popularity, bots within that environment will help automate meetings and status updates and so on, saving time and increasing productivity.

3. **Glitches:**

Expect to hear more about "glitches" in 2016. While there have always been software bugs, what we're seeing now is so much new technology coming online so quickly — without the usual testing — that we don't know what the interactions will be in advance.

In 2013, technical glitches caused a three-hour stop at the Nasdaq. Last year, a glitch caused 5,000 united flights to be grounded for two hours. Technical glitches halted trading at the New York Stock Exchange recently. Glitches cause temporary outages — and big headaches — for streaming providers such as Dish's Sling TV, which interrupted service during the premiere of *Walking Dead* spinoff *Fear the Walking Dead*. Glitches at Netflix have caused outages as well as strange mash up summaries for different films. A favorite: "Inspired by

Victor Hugo's novel, this Disney film follows a gentle, crippled bell ringer as he faces prejudice and tries to save the eyes of individual dinosaurs."

In many cases, glitches have to do with degraded network connectivity or a miscalculation of the bandwidth needed. But a lot of times, glitches have to do with newer technologies, which we are learning break in unexpected ways. Glitches aren't software bugs, which can be tested and rectified. Glitches are a newer phenomenon, which are difficult to predict in advance. This is not an argument against technology — it's a recommendation for increased systems monitoring and regular conversations with IT managers.

4. **Backdoors:**

Backdoors are lines of code developers intentionally install in firmware so that manufacturers can safely upgrade our devices and operating systems. It's a way for manufactures to get into your system to fix a problem without interrupting your experience. The challenge is that backdoors can also be used surreptitiously to harness everything from our webcams to our personal data.

Some government officials will be advocating for a set of "golden keys," which would allow law enforcement to use backdoors as they wish. This won't just affect the usual suspects, such as Facebook and Google. In 2016, any company that stores customer data could be asked to create a backdoor. This might include banks, advocacy groups, travel

agencies, hotel companies and more. Opponents argue that the simple act of creating a backdoor would leave ordinary people vulnerable to everyday attacks by even unskilled hackers. If your organization is approached next year, what will you do? Do you have a point of view and a plan to address backdoors?

5. **Blockchain:**

The blockchain is a sort of distributed consensus system, where no one person controls all the data. Thus far it's gotten the most press as the technology behind bitcoin, but everyone agrees that bitcoin probably isn't the blockchain's killer app. The cryptography team at Blockstream recently launched its first prototype "sidechain," which functions as a separate ledger with its own code. Sidechains allow for easier authentication. Blockstream and the sidechain projects that follow will turn the blockchain into a universal platform that can be used for anything requiring signatures or authentication. It will disrupt entire industries.

The blockchain enables people to participate in "trustless" transactions, eliminating the need for an intermediary between buyers and sellers. And it potentially eliminates the need for all intermediaries in most transactions, even those outside finance. The 21 Bitcoin Computer, is a small, bare bones, Linux-based piece of hardware in which the bitcoin protocol is a feature of the operating system. Any products or services built with it — games or music or any online

content—would have bitcoin built in as a component. It integrates bitcoin so seamlessly into devices that you'd never know that you're using the blockchain at all. It has the potential to eliminate thousands of intermediaries, such as payment services companies.

6. **Drone lanes:**

In 2015, two drones inadvertently prevented firefighters from putting out a rapidly spreading California wildfire, which crossed over onto a freeway and destroyed a dozen vehicles. Currently, the FAA does not allow drones to fly near the airspace of airports — but while there are no-fly zones, there aren't no-fly *circumstances*. From the Valley to DC, everyone will be talking in 2016 about whether or not the airspace should be regulated for hobbyists and commercial drone pilots, which will prompt difficult conversations between technologists, researchers, drone manufacturers, businesses and the aviation industry, since each has an economic stake in the future of unmanned vehicles. I anticipate the sky being divided soon: hobbyist pilots will have access to operate UMVs in the 200 and below space, while businesses and commercial pilots will gain exclusive access to 200–400 feet zone overhead.

7. **Quantum computing:**

In short, quantum computers can solve problems that are computationally too difficult for a classical computer, which can only process information in 1s and 0s. In the quantum universe, those 1 and 0 bytes can exist in two states (qubits) at once, allowing computations to be performed in parallel. Therefore, if you build two qubits, they are able to hold four values at the same time: 00, 01, 10, 11.

Quantum computers are not only more powerful than anything built to date — they require special algorithms capable of doing new things. For example, quantum computers require special programs like Shor's algorithm — invented by MIT's Peter Shor — that can factorize any prime number. The National Security Agency is already predicting that the cryptography in use will be rendered completely obsolete once quantum computers go into widespread use.

Scientists have been researching quantum computing for decades. The challenge has been proving that a quantum machine is actually doing quantum computations. That's because in a quantum system, the very act of observing information in transit changes the nature of that data. While you won't be able to buy a quantum computer in 2016, it's a trend worth watching. Researchers at IBM's experimental quantum computing group have begun to unlock difficult problems in quantum computing, such as detecting errors. Recently, D-Wave Systems announced that it broke the 1,000 qubit barrier, which (if true) would make it the most powerful computer on the planet. Now, IBM,

Microsoft, Hewlett-Packard and Google, as well as D-Wave, are trying to figure out how to advance and commercialize the technology.

8. **Augmented knowledge:**

We don't recognize it as such, but we are living in an age of digital telepathy, where we can send information directly to each other's brains via the internet. Scientists at the University of Southern California have been working on a cognitive neural prosthesis that can restore and enhance memory function. This research has a practical and altruistic purpose: to help victims of stroke or traumatic brain injuries regain their cognitive abilities and motor function. Rather than having to relearn, they need only reload those memories. But this implies that someday you might be able to augment your mental ability — much like robotic suits allow us to enhance our physical strength — with a computer device.

7. BADGE PROGRAM

Mr.P.Vignesh, II BCA 'A'

Linux Foundation tackles open source security with new badge program.

The Core Infrastructure Initiative's Best Practices Badge program will help businesses identify which open source projects follow a security-focused methodology.

Organizations have plenty of choices when looking at open source software, but the challenge lies in picking the right project to fit their needs. The CII Best Practices Badge program from the Linux Foundation's Core Infrastructure Initiative is intended to help organizations evaluate open source technologies based on security, quality, and stability.

Businesses increasingly rely on open source software, but they usually don't have a way to tell if developers are following secure coding practices, how they handle vulnerabilities and security updates, or how stable the software is. The CII Best Practices Badge program gives businesses answers to these questions.

"Giving people information about how the code is produced is much more valuable than saying, 'This specific version is secure,'" said Nicko van Someren, CTO of Linux Foundation.

The CII Best Practices Badge program does not designate specific products or software versions as being secure or free of vulnerabilities. Instead, the program asks open source project owners to provide information about how their projects are managed and how the software is being developed. Projects that pass -- are following best practices -- receive a badge to display on GitHub and elsewhere.

Inaugural badge holders include OpenSSL, Curl, GitLab, the Linux kernel, OpenBlox, Node.js, and Zephyr. CII's website has a searchable directory of open source projects that indicates whether they "pass" or

"fail" CII best practices. Projects will have to renew their qualifications on an ongoing basis to ensure they continue to receive pass ratings.

Open source project owners can sign up for the badging program and learn more about the criteria on the CII Best Practices page.

Organizations that rely on open source software can use the badges to identify projects which follow a security-focused methodology. Developers benefit from taking part in the CII Best Practices Badge program because they can quickly find out if their projects meet open source best practices. And if they fall short of badging requirements, they get feedback on what to fix.

"Open source projects often have very good security practices in place but need a way to validate those against industry and community best practices and ensure they're always improving," said Someren.

Like any open source initiative, the badge program needs the developer community to be involved. The program is led by David A. Wheeler, an open source and security research expert with the Institute for Defense Analyses (IDA), and Dan Kohn, a CII senior advisor. Even though the best practices developed by IDA aren't aligned against a specific framework or standard, there was a consensus on what should be included in the set, Someren said. And in cases where things don't quite match up, developers are encouraged to provide input so the program includes the most relevant criteria.

As more and more organizations rely on open source software, there are a lot of concerns about security. Much of the attention thus far has been on static and dynamic analysis – to uncover security vulnerabilities in code – and ensuring that developers use secure third-party libraries and components when writing code. Recently, the Underwriters Laboratories (UL) announced a Cybersecurity Assurance Program to test network-connected products for software vulnerabilities. Its badging program approaches software security from a different angle.

8. HOW TO MAKE ANDROID A REAL PART OF YOUR BUSINESS

R. Nirmala, Assistant Professor
Department of Computer Science

Over the past five years, iPhones and iPads have become the corporate mobile standards, thanks to their wealth of business apps, Exchange compatibility, corporate manageability, and strong security. Android devices, on the other hand, have largely been relegated to "OK for email" status.

But there's no longer a reason to keep Android at arm's length. It can now be as integral to your mobile portfolio as Apple's iOS devices are. Sure, Apple devices still lead in business-class apps, manageability, and security, but not by enough to exclude Android from full access at most companies.

With that in mind, InfoWorld has put together this guide on how to deploy Android, both for company-issued devices and BYOD scenarios; most companies likely have a mix of both approaches.

The Android devices you should support

Not all Android devices are created equal. For example, the cheapest devices rarely support encryption, so they're unsafe for corporate usage. Meanwhile, no-name Android devices are often infected with malware -- particularly devices sold in the developing world.

When it comes to Android devices, you should focus on the top-tier brands and models. The best options come from Samsung -- the Galaxy S and Galaxy Note lines of smartphones and the Galaxy Tab S series of tablets. Not only are they built to last, they support the widest range of

radio bands and have the best hardware-level security available. The Samsung devices also support the highest level of Android management.

If your security and management needs are not the most stringent -- that is, you're not a defense contractor or a government agency dealing with sensitive information, or you aren't focused on high-level corporate executives with sensitive company information -- there are plenty of other options, especially for smartphones from the best-known vendors, including LG, Lenovo's Motorola unit, Sony, Alcatel, and Google.

The second-tier providers typically support encryption and a broad swath of radio bands, as well as provide good fit and finish on their higher-end models.

What you won't get is the same level of hardware security as you do from Samsung. BlackBerry's Android smartphone, the Priv, which also has strong hardware-level security, may be an option for the more security-conscious, but the company's persistent market struggles should make you thinks twice about depending on it.

Stay away from most other companies, and be very cautious about Android devices bought in China, where it's quite likely the government has required backdoor access be installed.

Whatever you buy, try to choose a model no more than one generation old. Android makers and the carriers are very slow to update their devices, if they bother to update them at all. Anything older than last year's model is likely to not be updated -- not even for security. Plus, older models are less likely to support encryption and other hardware-based security features like fingerprint scanners.

Plan on two-year replacement cycles for Android devices that access sensitive information -- versus three or even four years for iOS devices. Apple is good about keeping old devices current via software updates, but Google and its Android allies are not.

For casual Android users -- those who use messaging, email, calendars, and perhaps Office, as well as have moderate information access permissions -- you can be more forgiving about device age.

The Android versions you should support

Android 4.4 KitKat is the oldest version your organization should support, as it was Android's first version to get management and security capabilities competitive with those found in iOS. If possible, restrict your usage to Android 5.0 Lollipop or later -- at least for users who work the most with sensitive information. Anything prior to Android 4.4 should be avoided.

Lollipop is the first Android version to support Google's Android for Work containers natively, and any company should use those containers or Samsung's own Knox for employees who deal with sensitive information (more on those shortly). Although Android for Work can be installed on some older Android versions, it's simply not as secure there.

The forthcoming Android N will broaden its focus into other enterprise features, such as multi-windowing, and offer additional management options. That's another reason to stick with recent-model devices: to increase the odds of supporting Android N next year.

Android management options you should consider

There are three levels of management available to you for Android devices, in addition to not managing them: basic Exchange management, server-based mobile management, and container-based separation.

Basic Exchange management: This option is essentially free if you use Microsoft Exchange. You set Exchange ActiveSync (EAS) policies to enforce basic security hygiene: require encryption be enabled, and require a password be enabled (and maybe even apply policies around password length, complexity, and/or expiration). More EAS policies are available, some of which would make sense for company-issued devices (such as disabling the camera or Wi-Fi), but that would be problematic for BYOD units because they restrict functionality that is perfectly acceptable -- and desirable -- outside of work.

Server-based mobile management: This option lets you manage more than EAS alone can. Like Apple, Google has developed a set of APIs for Android that allow third-party management servers to control the device. Some of these policies manage security settings, some control device configuration (such as locking a device to specific networks, requiring a corporate VPN be used, and whitelisting or blacklisting specific apps).

You should use such a server -- variably referred to by the acronyms MDM (Mobile Device Management) and EMM (Enterprise Mobility Management) -- at least for devices that you treat like computers. In other words, if a smartphone or tablet is used to run corporate apps, access

corporate servers beyond email and calendar, or interact with corporate data sets, treat it like a managed PC by using a management server.

The top providers are BlackBerry's Good Technology unit, Citrix Systems, EMC VMware's AirWatch unit, IBM's MaaS360 unit, MobileIron, and Soti. Microsoft is also stepping into this market as part of a broader push to converged mobile/PC management.

Using these management servers -- available via the cloud or on-premises servers -- will cost you anywhere from $3 to $20 per user per month, depending on how much you want to manage.

Be careful that you don't try to manage too much. As is typical in the security industry, mobile management vendors like to paint very scary pictures to up their sales, even though mobile devices are safer than PCs and are rarely the source of data breaches or viral infections. If you're securing your mobile devices more than your laptops, you're either overdoing it in mobile or falling short on your PCs.

One area where Android is at more risk than iOS is application security. Although Apple's App Store has seen malware get past Apple's defenses, it's rare, and the iOS architecture limits the potential damage. But Google's Play Store is more prone to having malware disguised as legitimate apps, and Android's architecture lets malware roam widely, similar to Windows. You should look seriously at using the mobile management server's application-management tools, which you've probably ignored if you're used to managing iOS.

But be careful about investing in antimalware apps for Android. It's not clear they catch much, and as we've seen on the desktop, they're pretty

much useless against phishing attacks, where the big breaches and attacks come. It's better to focus on using a policy to disallow "sideloaded" apps on managed Android devices, managing what apps can be installed, and focusing your security efforts on how your network and servers directly defend themselves against the attacks you know will come in from somewhere.

Container-based separation: Because Android has an open file system, data and malware can roam across the entire device. That's why first Samsung, then Google brought containers to the operating system level of Android, with their Knox and Android for Work offerings. (iOS uses sandboxes around each app, essentially putting each in its own container, with limited connection paths available for which there are also management tools to control.)

Containers essentially divide the device in two, with corporate apps, data, and services running in one secured container, and personal apps, data, and services running in another container. Some system functions, like the phone dialer, are available to both containers, but even in those cases the underlying data (like address books) can be kept separate.

The use of containers limits the potential for malware infection of corporate apps and the systems and data they access. It also protects users from IT snooping of their personal information. It also means a corporate wipe of a lost or stolen device won't wipe that personal portion. (Employees then have to wipe any sensitive personal information themselves, using a tool like Google's Android Device Manager, the Lookout software installed by several Android makers, or Samsung's own

Find My Mobile tool, all of which require employees to set up a corresponding personal account.)

Knox is older than Android for Work, but in reality, neither was up to snuff until 2015. Now that they are, you have to decide: Which one to use?

If you're an all-Samsung Android shop, go for Knox. It's natively supported by Samsung's higher-end recent devices and takes native advantage of Samsung's hardware security.

Otherwise, go for Android for Work. It's supported on most higher-end Android devices, including Samsung's.

In both cases, you oversee the containers' policies using a mobile management server. Not all vendors support Android for Work or Knox yet, but most of the top-tier ones do, including BlackBerry, Citrix, IBM, MobileIron, Soti, and VMware.

Again, avoid complex container "solutions" offered by mobile management vendors, such as app wrapping, proprietary containers, and proprietary apps that replace the native ones in Android (such as for email or browsing). These not only increase the costs, but increase the management overhead for IT. And frankly, the risks cited by most vendors are way overblown. It's a lot of money and effort for very little -- and often no -- additional real-world security.

The Android apps you should provide

Although iOS still rules in apps, Android now has the basics covered.

For office productivity, Microsoft Office is quite capable on Android -- and it's included with a corporate or personal Office 365 subscription. (In fact, a subscription is required to use more than the basic Office features.) No other office productivity suite comes close.

The Microsoft Outlook client for Android is OK for email and calendar access, but a better option is the set of Samsung apps that Galaxy users get with their device. Like Microsoft Outlook, Samsung's clients support both Exchange and non-Exchange accounts. Non-Galaxy users can use Google's merely adequate Gmail and Calendar apps -- or, better, start using Outlook.

If you're adopting cloud services to provide secure, managed, central storage for employee data, Android has clients for the major services that offer IT-managed versions: Box, Dropbox, Google Drive, and OneDrive. (Apple's iCloud Drive is not supported, but iCloud Drive isn't IT-manageable anyhow.)

And in addition to Android's built-in VPN client, you can get specialty Android VPN clients from Cisco and Juniper, if you use those VPNs' extra features. It's no longer true that Android devices must play second fiddle to iOS devices when it comes to such basic security and management tools.

Beyond that, you're talking domain-specific apps, which need to be tested in your environment and business context. Your IT mobile team should test out the clients (apps and Web) for any systems in place, from Workday to Oracle, from Jira to Salesforce -- travel expense managers, time

sheets, customer orders, operations dashboards, prospect management, and so on.

MAILING LIST – To Whom We Send

- **Mr.B.Murali, HOD of CS, PSG college of Arts and Science, Coimbatore- 14.**
- **Mr.P.Narendran, HOD of CS, Gobi Arts &Science College, Gobichettipalayam-53.**
- **Dr.M.Chandrasekharan, HOD of CS, Erode Arts College (Autonomous), Erode - 09.**
- **Mr.S.SureshBabu, HOD of CS, Thiruvalluvar Government Arts College, Rasipuram.**
- **Dr.K.Thangavel, HOD of CS, Periyar University, Salem-11.**
- **Prof S. Joseph Gabriel, HOD of CS, MazharulUloom College, Vellore – 02**
- **Dr.P.Venkatesan, Principal, Vysya College of Arts and Science, Salem-03,**

- **Dr.P.Swaminathan, Dean, School of Computing, SASTRA University, Kumbakonam.**
- **Dr.S.K.Jayanthi, HOD of CS, Vellalar College for Women, Erode-9**
- **Dr.S.Krishnamoorthy, Dean, Anna University, Trichy-24.**
- **Dr. K. Rama, Deputy Adviser, NAAC, Bangalore.**
- **Dr.HannahInbarani, Asst Prof, Dept of CS, Periyar University, Salem-11.**
- **Dr.R.Balasubramaniam, Prof& HOD of CS, ManonmaniamSundaranar University, Tirunelveli.**
- **Dr.P.Jaganathan, Director, Dept of MCA, PSNA Engineering College, Dindugal-22.**
- **Dr.D.Venkatesan, SeniorAsst. Prof, Dept. of CS, School of Computing, SASTRA University, Tanjore-01.**
- **Dr.C.Muthu, Reader, Dept of Information Science and Statistics, St. Joseph College, Tiruchirapalli– 02.**
- **Dr. D.I. George Amalarethinam, Director, Department of MCA, Jamal Mohamed College, Tiruchirapalli – 20.**
- **Mr. B. Rajesh Kanna, Assistant Professor in Elect &Comm, Annamalai University, Chidambaram.**
- **Dr.H.FaheemAhmed, Asst Prof & HOD of CS, Islamiah College, Vaniyambadi – 02**
- **Dr. S. Leela, Controller of Examination, Periyar University, Salem-11.**
- **Dr. M. Manivannan, The Registrar, Periyar University, Salem-11.**

- **Prof.Dr.C.Swaminathan, Vice Chancellor, Periyar University, Salem-11.**
- **Mr.Vaithiyanathan, Project Manager HCL Technologies, Chennai.**
- **Dr.T.Santhanam, Reader& HOD of CA, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai –06.**
- **Dr.SheelaRamachandran, Vice Chancellor, Avinashilingam University, Coimbatore.**
- **Dr.R.Rajesh, Asst. Prof, Dept of CS & Engineering, Bharathiyar University, Coimbatore – 46**
- **Dr.R.S.Rajesh, Reader, Computer Science and Engineering, ManonmaniamSundaranar University, Tirunelveli-12.**
- **Dr.L.Arockiam, Associate Professor, Dept of CS, St. Joseph College, Tiruchirapalli-620002**
- **Mr.V.Saravanan, Associate Professor, Dept of CA, Hindustan College of Arts and Science, Coimbatore – 28.**
- **Dr.R.Ravichandran, Secretary, Dept of CS, KGISL Institute of Technology, Coimbatore-35.**
- **Dr. N.Sairam, Associate Dean, School of Computing, Sastra University, Tanjore – 01**
- **Dr.T.Senthikumar, Asst Prof, Amrita Institute of Technology, Coimbatore - 12**
- **Mr.S.T.Rajan, Sr. Lectr, Dept of CS, St. Josephs College, Trichy-02.**
- **Dr.R.AmalRaj, Prof. Dept Of CS, SriVasavi College, Erode – 16.**
- **Dr. R. Pugazendi, Assistant Professor, Dept. of CS, Government Arts and Science College, Salem-7.**

WhatsApp

WhatsApp

Video Calling Activate

Now Whatsapp appm come up with one awesome lineament that is WhatsApp video calling feature.