DEPARTMENT OF INFORMATION TECHNOLOGY

Welcome to the Department of Information Technology.

As we all know, this is an era of Information Technology, and almost every one of us uses some kind of gadgets which invariably leverages the benefits of Information Technology. The advent of Information Technology has revolutionized the way we live. Moreover, Internet and mobile wireless technology are the boons of Information Technology. So, the department strives hard to groom our students with this cutting edge technology, thereby instilling high valued ethics and morals. The department prepares them to take up the challenges of ever changing dynamic IT industry.

To fulfill the vision and mission of Information Technology Department towards imparting quality education to our students we conduct various activities like expert lecture, seminar, workshop and industrial visit to make teaching process effective. We provide a platform to our students to participate in many extra-curricular activities through various technical, non- technical contests for their overall personality development.

All IndIA ShrI ShIvAjI MeMorIAl Society'S

Institute of Information Technology

Department of Information Technology

VISION

To equip students with core and state of the art Information Technology.

MISSION

Imparting knowledge of Information Technology and teaching its application through innovative practices and to instill high morale, ethics, lifelong learning skills, concern for the society and environment.

PROGRAM EDUCATION OBJECTIVES(PEO)

- To prepare graduates to solve multifaceted and complex problems in IT industries.
- To inculcate core professional skills with latest information technology to prepare graduates for employment and higher studies.
- To develop cross domain competences that prepares graduates for lifelong learning in diverse career paths.
- To make graduates aware of their social responsibilities toward environment and society.

PROGRAM SPECIFIC OUTCOMES(PSO)

- Graduates will be able to demonstrate database, networking and programming technologies.
- Graduates will be able to apply core, professional and state of the art Information Technology.

PROGRAM OUTCOMES(PO)

Graduates will be able to

- Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems. **[Engineering knowledge]**

- Identify, formulate, research literature and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and engineering sciences. **[Problem analysis]**

- Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety and cultural, societal and environmental considerations. **[Design/ development solutions]**

- Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of the information to provide valid conclusions. **[Conduct investigations of complex problems]**

- Create, select and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations. **[Modern tool usage]**

- Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. **[The engineer and society]**

- Understand the impact of the professional engineering solutions in societal and environmental contexts and demonstrate the knowledge of, and need for sustainable development. **[Environment and sustainability]**
- Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. **[Ethics]**

- Function effectively as an individualand as a member or leader in diverse teams and in multidisciplinary settings. **[Individual and team work]**

- Communicate effectively on complex engineering activities with the engineering community and with society at large such as, being able to comprehend and write effective reports and design documentation, make effectivepresentations and give and receive clear instructions. **[Communication]**

- Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team to manage projects and in multidisciplinary environments. **[Project management and finance]**

- Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. **[Lifelong learning]**

Message from HOD

It is a great privilege and immense honor to inform you that the Department of Information Technology is publishing its 6th annual technical magazine "**Eminence-2k19**".It is reflection of student's hidden talents, skills and caliber. This magazine certainly would induce the young engineers to promote their creativity in approaching things differently.

This technical magazine is a platform to exhibit the literary skills and innovative ideas of students. Through this magazine students can convey inspirational articles, vibrant drawings, mind-scintillating poems and updates of current trends to others.

All these things have been made possible by the extraordinary vision of Shri Malojiraje Chhatrapati, Hon.Secretary, All India Shri Shivaji Memorial Society and the immaculate planning of Dr.P.B.Mane, Principal All India Shri Shivaji Memorial Society Institute of Information Technology.

I take this opportunity to congratulate the chief editor Prof. Mrs. R.P. Saste for bringing out this magazine as per schedule, which in itself is an achievement considering the effort and time required. I would like to thank all editorial team members for providing students a platform for creative thoughts and knowledge expansion. I express my considerable appreciation to all the authors of the articles in this magazine. I express my gratitude to all for their involvement, encouragement, support and guidance.

Dr. Meenakshi A Thalor
HOD-IT Department
AISSMS IOIT,Pune

Message from EDITOR

I proudly present 6th successive edition of our department's annual technical magazine **"Eminence-2k19"**.

This year we are showcasing innovative ideas and hidden talents of our young minds on the theme "Android & iOS". The objective of the magazine is to provide platform for our students to augment the technology focus and scope of it.The technical section of this magazine elaborates importance of Android and iOS in the field of communication .Over the years, communication methods have evolved from simple text messages and audio calls to more efficient video calls and chat platforms which offer other communication services. The impact of technology in communication has influenced both individuals and businesses.

On behalf of the entire magazine team I would like to extend my gratitude to our respected Principal Dr. P.B. Mane and HOD Dr. M. A. Thalor for their invaluable guidance and support towards accomplishment of ITSA events successfully.

Special thanks to team of enthusiastic and dynamic students for their incredible contribution in making of the magazine. There is remarkable contribution of the student's editorial team to make this magazine amazing. I congratulate all the participants for sharing notable articles in the magazine.

Mrs. Rasika P. Saste
Chief Editor and Magazine Coordinator
Assistant Professor
Department of Information Technology

EDITORIAL TEAM

Technical Magazine Team Members (L-R):

Revati Awale (B.E)
Jignesh C Tanna (B.E)

MESSAGE FROM EDITORIAL TEAM

It has become appallingly obvious that our technology has exceeded our humanity.

- Albert Einstein

We take it in oUR pride to present to yoU the 6th edition of technical magaZine ***"Eminence 2k19"***

This issUE will take yoU throUGH the technological advancements in space sciences and globally evolving technologies.

This tech-croZier is a collection of a perfect balance of technology, knowledge, creativity and expression- exactly what we ENGINEERs are made of!

Rendering throUGH the magaZine will take yoU throUGH the ennoblement of Android and its FeatUREs along with the breakthroUGH of IOS in new era of the Information Technology.

We hope this edition serves to enlighten and gladden all the readers.

Feedback has always been the breakfast of the champions.

Good feedback will give Us the oppoRTUnity to improve; hence any sUGGestions are always welcome!

Mail Us at:*itsa.technicalmag@gmail.com*

INDEX

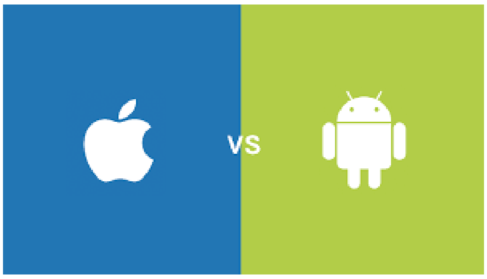
IOS VS ANDROID

iOS

The original iPhone operating system was simply called iPhone OS in 2007 but was renamed to iOS a few years later. At launch, it boasted a few apps like Mail, iPod, Calendar, Photos, Clock but no App Store. The first iOS SDK was released in 2008, paving the way for thousands of apps supported on the iPhone today. In the same year, iOS 2.0 was released with the App Store which pushed the iPhone years ahead of the competition. Cut, copy and paste came with iOS 3.0 in 2009, Facetime in iOS 4 (2010), with continuous improvements until iOS7 in 2013. With iOS 7, the UI made a major change. Gone were the rich glossy textures and skeuomorphic UI elements replaced by the flatter graphics and colourful gradients.

The iOS user interface is based upon direct manipulation, using multi-touch gestures. Interface control elements consist of sliders, switches, and buttons. Interaction with the OS includes gestures such as *swipe*, *tap*, *pinch*, and *reverse pinch*, all of which have specific definitions within the context of the iOS operating system and its multi-touch interface. Internal accelerometers are used by some applications to respond to shaking the device (one common result is the undo command) or rotating it in three diamensions(one common result is switching between portrait and landscape mode). Apple has been significantly praised for incorporating thorough accessibility functions into iOS, enabling users with vision and hearing disabilities to properly use its products.

Major versions of iOS are released annually. The current version,iOS12, was released on September 17, 2018. It is available for all iOS devices with 64-bit processors; the iPhone 5S and later iPhone models, the iPad 2017, the iPad Air and later iPad Air models, all iPad Pro models, the iPad Mini 2, and later iPad Mini models, and the sixth generation iPad-touch. On all recent iOS devices, iOS regularly checks on the availability of an update, and if one is available, will prompt the user to permit its automatic installation.



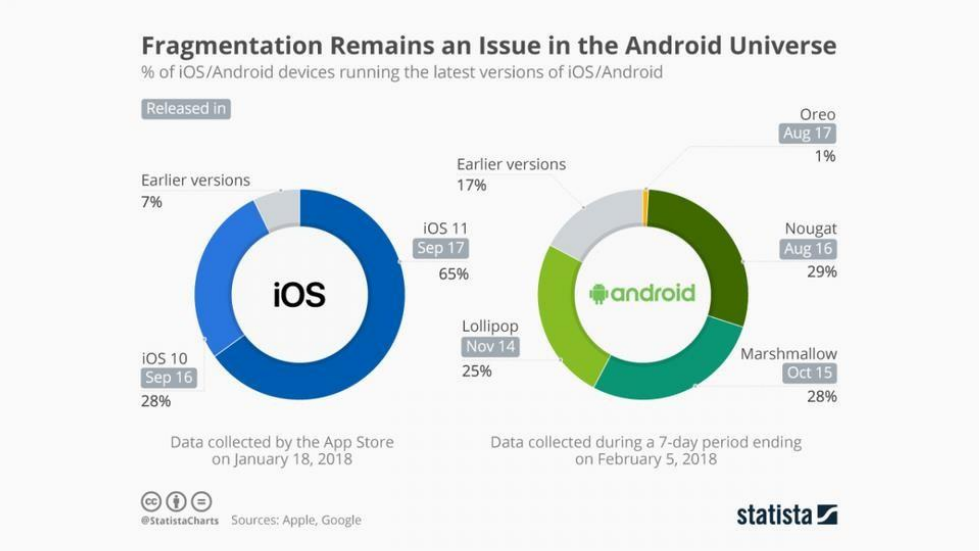
Android

Android 1.0 was released in 2008 and was lacking in many core features such as media player, camcorder and proper Bluetooth support. The first major update came as Android 1.5 Cupcake, which started the whole dessert naming convention. HTC Magic, the first touch-screen only Android phone, gave us a universal search box, screen rotation, deleting of multiple photos, copy & paste, widgets and improved camera app. As time passes, new updates provided more features with increased screen sizes and more powerful hardware. They sported names like Donut (1.6), Éclair (2.0/2.1), Froyo (2.2), Gingerbread (2.3), Honeycomb (3.0/3.1/3.2), Ice Cream Sandwich (4.0), Jelly Bean (4.1/4.2/4.3) and KitKat (4.4) in 2013.

The current stable version is Android 9 “Pie”, released in August 2018. Google released the first beta of the next release, Android 10 (code-named Android Q during development), on Pixel phones in March 2019. The core Android source code is known as Android Open Source Project (AOSP), which is primarily licensed under the Apache License

Android is also associated with a suite of proprietary software developed by Google, called Google Mobile Services (GMS), that frequently comes pre-installed on devices. This includes core apps such as Gmail, the application store / digital distribution platform Google Play and associated Google Play Services development platform, and usually includes the Google Chrome web browser and Google Search app.

Android has been the best-selling OS worldwide on smartphones since 2011 and on tablets since 2013. As of May 2017, it has over two billion monthly active users the largest installed base of any operating system, and as of December 2018, the Google Play store features over 2.6 million apps.



Revati Awale
BE IT

iOS Versions

iOS is the name of the operating system that runs the iPhone, iPod touch, and iPad. It's the core software that comes loaded on all devices to allow them to run and support other apps. The iOS is to the iPhone what Windows is to PCs or macOS is to Macs.

Below you'll find a history of each version of the iOS when it was released, and what it added to the platform. Click the name of the iOS version, or the More link at the end of each blurb, for more in-depth information about that version.

iOS 1

The one that started it all, which shipped pre-installed on the original iPhone. This version of the operating system wasn't called the iOS at the time it launched. From versions 1-3, Apple referred to it as the iPhone OS. The name shifted to iOS with version 4. It's hard to convey to modern readers who have lived with the iPhone for years how profound a breakthrough this version of the operating system was. Support for features like the multitouch screen, Visual Voicemail, and iTunes integration were significant advances. While this initial release was a major breakthrough at the time, it lacked many of the features that would come to be closely associated with the iPhone in the future, incuding support for native, third-party apps. Pre-installed apps included Calendar, Photos, Camera, Notes, Safari, Mail, Phone, and iPod (which was later split into the Music and Videos apps). Version 1.1, which was released in Sept. 2007 was the first version of the software compatible with the iPod touch.

Digital currencies are intangible and can only be owned and transacted in by using computers or electronic wallets which are connected to the Internet or the designated networks. In contrast, the physical currencies, like bank notes and minted coins, are tangible and transactions are possible only by their holders who have their physical ownership.

iOS 2

One year after the iPhone became a bigger hit than almost anyone projected, Apple released iOS 2.0 (then called iPhone OS 2.0) to coincide with the release of the iPhone 3G.

The most profound change introduced in this version was the App Store and its support for native, third-party apps. Around 500 apps were available in the App Store at launch. Hundreds of other crucial improvements were also added.

Other important changes introduced in the 5 updates iPhone OS 2.0 included podcast support and public transit and walking directions in Maps (both in version 2.2).

Key New Features: 1) App Store 2)Improved Maps app

iOS 3

The release of this version of the iOS accompanied the debut of the iPhone 3GS. It added features including copy and paste, Spotlight search, MMS support in the Messages app, and the ability to record videos using the Camera app.

Also notable about this version of the iOS is that it was the first to support the iPad. The 1st generation iPad was released in 2010, and version 3.2 of the software came with it.

Key New Features: 1) Copy and paste 2) Spotlight search 3)Recording videos

iOS 4

Many aspects of the modern iOS began to take shape in iOS 4. Features that are now widely used debuted in various updates to this version, including FaceTime, multitasking, iBooks, organizing apps into folders, Personal Hotspot, AirPlay, and AirPrint.

Another important change introduced with iOS 4 was the name "iOS" itself. As noted earlier, the iOS name was unveiled for this version, replacing the previously used "iPhone OS" name.

This was also the first version of the iOS to drop support for any iOS devices. It was not compatible with the original iPhone or the 1st generation iPod touch. Some older models that were technically compatible were not able to use all features of this version.

Key New Features:1) FaceTime 2)Multitasking 3)Air Play 4)Air Print 5)Personal Hotspot

iOS 5

Apple responded to the growing trend of wirelessness, and cloud computing, in iOS 5, by introducing essential new features and platforms. Among those was iCloud, the ability to activate an iPhone wirelessly (previously it had required a connection to a computer), and syncing with iTunes via Wi-Fi.

More features that are now central to the iOS experience debuted here, including iMessage and Notification Center.

With iOS 5, Apple dropped support for the iPhone 3G, 1st gen. iPad, and 2nd and 3rd gen. iPod touch.

Key New Features:1) iCloud 2)iMessage 3)Notification Center 4)Wireless syncing and activation

iOS 6

Controversy was one of the dominant themes of iOS 6. While this version introduced the world to Siri — which, despite being later surpassed by competitors, was a truly revolutionary technology — problems with it also led to major changes.

The driver of these problems was Apple's increasing competition with Google, whose Android smartphone platform was posing a threat to the iPhone. Google had supplied the Maps and YouTube apps pre-installed with the iPhone since 1.0. In iOS 6, that changed.

Apple introduced its own Maps app, which was badly received due to bugs, bad directions, and problems with certain features. As part of the company's efforts to solve the problems, Apple CEO Tim Cook asked the head of iOS development, Scott Forstall, to make a public apology. When he refused, Cook fired him. Forstall had been involved with the iPhone since before the first model, so this was a profound change.

Key New Features:1) Apple Maps 2)Do Not Disturb 3)Passbook (now Wallet)

iOS 7

Like iOS 6, iOS 7 was met with substantial resistance upon its release. Unlike iOS 6, though, the cause of unhappiness among iOS 7 users wasn't that things didn't work. Rather, it was because things had changed.

After the firing of Scott Forstall, iOS development was overseen by JonyIve, Apple's head of design, who had previously only worked on hardware. In this version of the iOS, Ive ushered in a major overhaul of the user interface, designed to make it more modern.

Key New Features:1) Activation Lock 2)AirDrop 3)CarPlay
4)Control Center 5)Touch ID

iOS 8

More consistent and stable operation returned to the iOS in version 8.0. With the radical changes of the last two versions now in the past, Apple once again focused on delivering major new features.

Among these features was its secure, contactless payment system Apple Pay and, with the iOS 8.4 update, the Apple Music subscription service.

There were continued improvements to the iCloud platform, too, with the addition of the Dropbox-like iClould Drive, iCloud Photo Library, and iCloud Music Library.

Key New Features:1) Apple Music 2)Apple Pay 3)iCloud Drive 4)Handoff
5)Family Sharing 6)Third-party keyboards 7)HomeKit

iOS 9

After a few years of major changes to both the interface and technical foundation of the iOS, many observers began to charge that the iOS was no longer the stable, dependable, solid performer it had once been. They suggested that Apple should focus on shoring up the foundation of the OS before adding new features.

That's just what the company did with iOS 9. While it did add some new features, this release was generally aimed at solidifying the foundation of the OS for the future.

Major improvements were delivered in speed and responsiveness, stability, and performance on older devices. iOS 9 proved to be an important refocusing that laid the groundwork for the bigger improvements delivered in iOS 10 and 11.

Key New Features:1) Night Shift 2)Low Power Mode 3)Public beta program

iOS 10

The ecosystem that Apple built around the iOS has long been referred to as a "walled garden" because it's a very pleasant place to be on the inside, but it's hard to gain access to. This was reflected in the many ways Apple locked down the interface of the iOS the options it gave to apps.

Cracks begin to show in the walled garden in iOS 10, and Apple put them there. The major themes of iOS 10 were interoperability and customization. Apps could now communicate directly with each other on a device, allowing one app to use some features from another without opening the second app. Siri became available to third-party apps in new ways.

Beyond that, users now had new ways to customize their experiences, from (finally!) being able to delete built-in apps to new animations and effects to punctuate their text messages.

Key New Features:1)iMessage apps 2)Delete built-in apps

iOS 11

The iOS was originally developed to run on the iPhone. Since then, it's been expanded to support the iPod touch and iPad (and versions of it even power the Apple Watch and Apple TV). In iOS 11, the emphasis shifted from the iPhone to the iPad.

Sure, iOS 11 contains lots of improvements for the iPhone, but its major focus is turning the iPad Pro series models into legitimate laptop replacements for some users.

Key New Features:1) Augmented Reality 2)AirPlay 2 3)Major enhancements on iPad

iOS 12

The new features and improvements added in iOS 12 aren't as extensive or revolutionary as in some previous updates to the OS. Instead, iOS 12 focused more on making refinements to commonly used features and on adding wrinkles that improve how people use their devices.

Some of the key features of iOS 12 included improvements to Siri like Siri Shortcuts, enhanced Augmented Reality with ARKit 2, and giving users and parents ways to monitor and control their device use with Screen Time.

Key New Features:1) Grouped Notifications 2) Screen Time 3)ARKit 2 4)Siri improvements, including Siri Shortcuts and multi-step actions 5)Memoji, a personalized kind of Animoji

iOS 13

It will be released in Fall 2019. Perhaps the biggest change introduced with iOS 13 is that the OS no longer runs on the iPad. That's due to the release of iPadOS (which begins with version 13). That's a new OS dedicated to making the iPad a more useful productivity device and a potential laptop replacement. It's based on iOS 13 and has many of the same features, but also adds iPad-specific items. Beyond that, iOS 13 shores up some core features, including launching apps faster, unlocking devices with Face ID faster, and overhauling pre-installed apps like Reminders, Notes, Safari, and Mail. Maybe the most obvious new feature is the Dark Mode, but the changes range much wider than that and further bolster the already-strong OS.

Key New Features:1) System-wide Dark Mode 2)Sign In With Apple user account system 3) New privacy and security options 4)New Portrait Lighting options 5)Look Around, a Google Street View-style feature for Apple Maps 6)New, improved Siri voice 7) Overhauled stock apps like Reminders and Notes

Jignesh Tanna
BE IT

Android Versions

What a long, strange trip it's been.

From its inaugural release to today, Android has transformed visually, conceptually and functionally — time and time again. Google's mobile operating system may have started out scrappy, but holy moly, has it ever evolved.
Here's a fast-paced tour of Android version highlights from the platform's birth to present.

Android versions 1.0 to 1.1: The early days

Android made its official public debut in 2008 with Android 1.0 — a release so ancient it didn't even have a cute codename.
Things were pretty basic back then, but the software did include a suite of early Google apps like Gmail, Maps, Calendar, and YouTube, all of which were integrated into the operating system — a stark contrast to the more easily updatable standalone-app model employed today.

Android version 1.5: Cupcake

With early 2009's Android 1.5 Cupcake release, the tradition of Android version names was born. Cupcake introduced numerous refinements to the Android interface, including the first on-screen keyboard — something that'd be necessary as phones moved away from the once-ubiquitous physical keyboard model.
Cupcake also brought about the framework for third-party app widgets, which would quickly turn into one of Android's most distinguishing elements, and it provided the platform's first-ever option for video recording.

Android version 1.6: Donut

Android 1.6, Donut, rolled into the world in the fall of 2009. Donut filled in some important holes in Android's center, including the ability for the OS to operate on a variety of different screen sizes and resolutions — a factor that'd be critical in the years to come. It also added support for CDMA networks like Verizon, which would play a key role in Android's imminent explosion.

Android versions 2.0 to 2.1: Eclair

Keeping up the breakneck release pace of Android's early years, Android 2.0 Eclair, emerged just six weeks after Donut; its "point-one" update, also called

Eclair, came out a couple months later. Eclair was the first Android release to enter mainstream consciousness thanks to the original Motorola Droid phone and the massive Verizon-led marketing campaign surrounding it.

The release's most transformative element was the addition of voice-guided turn-by-turn navigation and real-time traffic info — something previously unheard of (and still essentially unmatched) in the smartphone world. Navigation aside, Eclair brought live wallpapers to Android as well as the platform's first speech-to-text function. And it made waves for injecting the once-iOS-exclusive pinch-to-zoom capability into Android — a move often seen as the spark that ignited Apple's long-lasting "thermonuclear war" against Google.

Android version 2.2: Froyo

Just four months after Android 2.1 arrived, Google served up Android 2.2, Froyo, which revolved largely around under-the-hood performance improvements.

Froyo did deliver some important front-facing features, though, including the addition of the now-standard dock at the bottom of the home screen as well as the first incarnation of Voice Actions, which allowed you to perform basic functions like getting directions and making notes by tapping an icon and then speaking a command.

Notably, Froyo also brought support for Flash to Android's web browser — an option that was significant both because of the widespread use of Flash at the time and because of Apple's adamant stance against supporting its on its own mobile devices. Apple would eventually win, of course, and Flash would become far less common. But back when it was still everywhere, being able to access the full web without any black holes was a genuine advantage only Android could offer.

Android version 2.3: Gingerbread

Android's first true visual identity started coming into focus with 2010's Gingerbread release. Bright green had long been the color of Android's robot mascot, and with Gingerbread, it became an integral part of the operating system's appearance. Black and green seeped all over the UI as Android started its slow march toward distinctive design.

Android 3.0 to 3.2: Honeycomb

2011's Honeycomb period was a weird time for Android. Android 3.0 came into the world as a tablet-only release to accompany the launch of the Motorola Xoom, and through the subsequent 3.1 and 3.2 updates, it remained a tablet-exclusive (and closed-source) entity.

Under the guidance of newly arrived design chief Matias Duarte, Honeycomb introduced a dramatically reimagined UI for Android. It had a space-like "holographic" design that traded the platform's trademark green for blue and placed an emphasis on making the most of a tablet's screen space.

While the concept of a tablet-specific interface didn't last long, many of Honeycomb's ideas laid the groundwork for the Android we know today. The software was the first to use on-screen buttons for Android's main navigational commands; it marked the beginning of the end for the permanent overflow-menu button; and it introduced the concept of a card-like UI with its take on the Recent Apps list.

Android version 4.0: Ice Cream Sandwich

With Honeycomb acting as the bridge from old to new, Ice Cream Sandwich — also released in 2011 — served as the platform's official entry into the era of modern design. The release refined the visual concepts introduced with Honeycomb and reunited tablets and phones with a single, unified UI vision.

ICS dropped much of Honeycomb's "holographic" appearance but kept its use of blue as a system-wide highlight. And it carried over core system elements like on-screen buttons and a card-like appearance for app-switching.

Android 4.0 also made swiping a more integral method of getting around the operating system, with the then-revolutionary-feeling ability to swipe away things like notifications and recent apps. And it started the slow process of bringing a standardized design framework — known as "Holo"— all throughout the OS and into Android's app ecosystem.

Android versions 4.1 to 4.3: Jelly Bean

Spread across three impactful Android versions, 2012 and 2013's Jelly Bean releases took ICS's fresh foundation and made meaningful strides in fine-tuning and building upon it. The release added plenty of poise and polish into the operating system and went a long way in making Android more inviting for the average user.

Visuals aside, Jelly Bean brought about our first taste of Google Now — the spectacular predictive-intelligence utility that's sadly since devolved into a glorified news feed.

Android version 4.4: KitKat

Late-2013's KitKat release marked the end of Android's dark era, as the blacks of Gingerbread and the blues of Honeycomb finally made their way out of the operating system. Lighter backgrounds and more neutral highlights took their places, with a transparent status bar and white icons giving the OS a more contemporary appearance.

Android 4.4 also saw the first version of "OK, Google" support — but in KitKat, the hands-free activation prompt worked only when your screen was already on *and* you were either at your home screen or inside the Google app.

The release was Google's first foray into claiming a full panel of the home screen for its services, too — at least, for users of its own Nexus phones and those who chose to download its first-ever standalone launcher.

Android versions 5.0 and 5.1: Lollipop

Google essentially reinvented Android — again — with its Android 5.0 Lollipop release in the fall of 2014. Lollipop launched the still-present-today Material Design standard, which brought a whole new look that extended across all of Android, its apps and even other Google products.

The card-based concept that had been scattered throughout Android became a core UI pattern — one that would guide the appearance of everything from notifications, which now showed up on the lock screen for at-a-glance access, to the Recent Apps list, which took on an unabashedly card-based appearance.

Lollipop introduced a slew of new features into Android, including truly hands-free voice control via the "OK, Google" command, support for multiple users on phones and a priority mode for better notification management.

Android version 6.0: Marshmallow

In the grand scheme of things, 2015's Marshmallow was a fairly minor Android release — one that seemed more like a 0.1-level update than anything deserving of a full number bump. But it started the trend of Google releasing one major Android version per year and that version always receiving its own whole number.

Marshmallow's most attention-grabbing element was a screen-search feature called Now On Tap — something that, as I said at the time, had tons of potential that wasn't fully tapped. Google never quite perfected the system and ended up quietly retiring its brand and moving it out of the forefront the following year.

Android 6.0 did introduce some stuff with lasting impact, though, including more granular app permissions, support for fingerprint readers, and support for USB-C.

Android versions 7.0 and 7.1: Nougat

Google's 2016 Android Nougat releases provided Android with a native split-screen mode, a new bundled-by-app system for organizing notifications, and a Data Saver feature. Nougat added some smaller but still significant features, too, like an Alt-Tab-like shortcut for snapping between apps.

Perhaps most pivotal among Nougat's enhancements, however, was the launch of the Google Assistant — which came alongside the announcement of Google's first fully self-made phone, the Pixel, about two months after Nougat's debut. The Assistant would go on to become a critical component of Android and most other Google products and is arguably the company's foremost effort today.

Android version 8.0 and 8.1: Oreo

Android Oreo added a variety of niceties to the platform, including a native picture-in-picture mode, a notification snoozing option, and notification channels that offer fine control over how apps can alert you.

The 2017 release also included some noteworthy elements that furthered Google's goal of aligning Android and Chrome OS and improving the experience of using Android apps on Chromebooks, and it was the first Android version to feature Project Treble — an ambitious effort to create a modular base for Android's code with the hope of making it easier for device-makers to provide timely software updates.

Android version 9: Pie

The freshly baked scent of Android Pie, a.k.a. Android 9, wafted into the Android ecosystem in early August 2018. Pie's most transformative change was its new gesture navigation system, which traded Android's traditional Back, Home, and Overview keys for a large, multifunctional Home button and a series of gesture-based commands.

Pie included some noteworthy new productivity features, too, such as a universal suggested-reply system for messaging notifications, a more effective method of screenshot management, and more intelligent systems for power management and screen brightness control.Android 9 had plenty of under-the-hood improvements as well, including a variety of privacy and security enhancements. Pie also introduced a new dashboard of "Digital Wellbeing" controls intended to help with the ever-present challenge of balancing the digital and physical world.

Mayur Dokras
BE IT

Programming language Dictionary

- A - Arithmetic language developed by Grace Hopper in 1951.
- B - Bell labs is a programming language developed at Bell labs circa 1969.
- General purpose computer programming language developed by Dennis Ritchie in 1969.
- D - Object-oriented multi-paradim system programming language.
- E - Object-oriented programming language for secure distributed computing, developed by Mark S Miller, Dan Bornsen, in 1997.
- F - Module-oriented, compiled and numeric computer programming developed for scientific programming and scientificcomputation.
- G - Numerical Control(NC)programming language. It is used mainly in computer-aided manufacturing for controlling automated machine tools.
- H - Hack is a programming language for the Hip Hop Virtual Machine(HHVM), created by Facebook as a dialect of PHP.
- Interactive Data Language (IDL), is a programming language used for data analysis. It is popular in particular areas of science, such as astronomy, atmospheric and medical imaging.
- J-Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented,platformed independent language.
- K-Is a proprietary array processing language developed by Arthur Whitney and commercialized by Kx Systems.
- L- Larry McAvoy, with extensive help from Jeffrey Hobbs, Oscar Bonilla.
- M-MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and 4th generation programming language.
- N– Net Logo is an agent-based programming language designed foe logo programming. Programming language Dictionary 3
- O-Oak is a programming language created by James Gosling in 1991 Sun Microsystems set-top box project.
- P- Perl (PracticalExtraction and ReportingLanguage) is a family of high-level, generalpurpose,interpreted, dynamic programming language.
- Q- Proprietary array processing language developed by Arthur Whitneyand commercialized by Kxsystems .
- R- Programming language and software environment for statisticalcomputing and graphics.
- S- Is a statistical programming language developed primarily by John Chambers Rick Becker and Allan Wilks of Bell laboratories.

- T- Programming language is a dialect of the Scheme programming language developed in the early 1980s by Jonathan A. Rees, Kent M. Pitman, and Norman I.
- U- Ubercode is a high level programming languagedeveloped by UbercodeSoftware and in 2005 for Microsoft Windows.
- V- VHDL (VHSIC Hardware Description Language) is a hardware description language used in electronic design automation to describe digital and mixed-signals systems.
- W- WATFIV developed at the University of waterloo is an implementation of the FORTRAN programming language.
- X- XBL (XML Binding Language) is an XML-based mark-up language used to declare the behaviour and look of XUL-widgets and XML elements.
- Y- Yahoo Query Language (YQL) is an SQL like query language created by Yahoo as part of their Developer Network . YQL is designed to retrieve and manipulate data from single Web interface
- Z- Z notation is a formal specification language used for describing and modelling computing systems..

Jignesh Tanna
BE IT

Artificial Intelligence

(AI) is one of the biggest technology trends of recent years. AI is transforming everything from marketing to shopping to online gaming. Businesses are finding many creative ways to utilize artificial intelligence, such as chatbots to enhance customer service and tools for marketing automation. Another overlooked area that AI can help businesses is by making life easier for employees. Let's explore some of the ways AI for workplace apps can enhance the internal operations of your business.

❖ IMPROVING RECRUITMENT AND EMPLOYEE ONBOARDING

AI can make life easier for both recruiters and job applicants. Furthermore, it can simplify the onboarding experience for new recruits. These possibilities are already being realized by many companies, especially in the hospitality industry. For example, Marriott International uses an innovative chatbot for Facebook Messenger that makes it easier for candidates to learn more about career opportunities. These types of tools help to attract better targeted and betterinformed candidates and take a load off HR departments. Artificial intelligence can also improve onboarding and training. For example, the AI training tool Chorus listens to sales calls and is able to offer suggestions to improve results. As AI gets more advanced, there will be more and more ways that it helps with training.

❖ BOOST PRODUCTIVITY

Workplace apps are already enhancing productivity, allowing for the automation of many everyday tasks. AI has the potential to take this a step further. Every business has tedious administrative tasks that add up to many hours in a week. AI software, such as automated personal assistants, can help to perform many related tasks. For example, when it comes to organizing a meeting, AI could interface with your scheduling apps (e.g. Slack) and save people from having to make lots of phone calls or send out multiple emails.

❖ ENHANCE COMMUNICATIONS

Modern business depends heavily on effective communication, both internally and externally. As noted, AI can help with tasks such as planning meetings. It can even help you communicate with people around the world who speak different languages. For example, Skype Translator is a multilingual AI assistant that can be used in conference calls. This futuristic software supports 10 languages for voice and 60 with text, making it possible to communicate normally with people who couldn't otherwise understand one another. The age of artificial intelligence is just beginning and has been noted as a technology on the rise in 2018. No doubt, there will be numerous ways to incorporate AI for workplace apps and other essential everyday responsibilities. Businesses will be able to free up time and handle many tasks more efficiently. This will benefit management, employees and customers alike.

Arnav Deshmukh & Pranav Deshmukh
BE IT

CRYPTOCURRENCIES

As cryptocurrencies are still a relatively new introduction to the world, concerns about security introduce a degree of risk into this payment system.

Cybercriminals are working relentlessly to find ways to take advantage of this new technology and exploit cryptocurrencies for their own financial gain and to access and acquire the data flowing through this newer payment system. For this reason, you might be thinking, “is cryptocurrency safe?” And, “what can I do to protect my investment?”

Since the introduction of Bitcoin in 2009, which is generally considered the first decentralized cryptocurrency, over 4,000 variations of cryptocurrency have been created worldwide. Bitcoin itself has never been compromised to date, so the coins themselves and the Bitcoin alternatives are considered safe and secure. However, cryptocurrency exchanges have been hacked and individuals’ accounts have been compromised –resulting in hundreds of millions of dollars in cryptocurrency being stolen. Phishing, malware and ransomware are common tactics used by cybercriminals to mine for cryptocurrency. These tactics exploit vulnerabilities in the exchanges, access cryptocurrency wallets and exploit third-parties that are connected to this payment system.

There are four ways to protect your cryptocurrency investment and enhance security by using features built into the currencies or the networks they run on.

1. **Avoid Cryptocurrency Scams**

There are currently over a 1,000 Active Cryptocurrencies on the market, and many come and go each month. Some of these are nothing more than just an online Bitcoin scam used as a way to pilfer coins from unsuspecting investors. One of the common ways fraudsters scam cryptocurrency users is by advertising a new coin and building up interest. Next, they offer an initial coin offering (ICO). Before users notice something has gone wrong, the fraudsters have pocketed the cryptocurrencies, and the site and the coin have vanished. Because of these 12th Annual Taste of IT Conference - #TOIT18 Wednesday, November 14 Sinclair College Ponitz Center 444 W Third St, Dayton, OH 45402scams, a great deal of research should be done to find a currency with a solid background.

2. **Secure Crypto Wallets**

When investing or applying cryptocurrencies for use, it is necessary to store cryptocurrencies in a secure wallet. Although there are hot wallets which are ideal for usability, hot wallets can be hacked. Cold wallets are the most secure. There are two types of cold storage wallets to choose from: paper and hardware. A paper wallet may be one of the simplest, but your keys are printed to paper, which is not the safest medium. The hardware wallet, which is much the same as a USB drive, is the more secure cold storage option. Not only is it more secure, it can also support many varying types of cryptocurrency. A prime example of the best is the Trezor hardware wallet. This comes with 2-factor authentication, and password manager –should the device be damaged, lost or stolen.

3. Cryptocurrency Exchange Theft

Cryptocurrency exchanges exist around the globe, though many of these are not the ideal places to leave your coins. When looking at which cryptocurrency to invest in the chosen must be considered. Up until recently, Mt. Gox was the most well-known exchange to be hacked. Over $450 million worth of Bitcoin was stolen from their Hot Wallet over a period of time. This shows how crucial it is to conduct due diligence on the exchange, and never leave your coins in any one exchange for any length of time.

4. How Crypto Coins Help Secure Your Investment

Many security weaknesses and fraudulent breaches happen at the exchange level, the wallet level, or other third-party level. Many cryptocurrencies

Swarali Shah & Riya Jain
BE IT

Your Robot Coworker – The Rise of Everyday AI& Automation

In the heady and hype-filled world of Artificial Intelligence, it can be hard to separate fact from (science) fiction. We hear of all the ways AI will transform our professional and personal lives, but as we head into 2019, it seems our lives remain largely untouched by AI outside of the usual suspects like Netflix, Alexa, and driverless cars. Or is that really the case?

Consider just a few of the recent advancements in "everyday AI": intelligent machines working behind the scenes to automate and improve your day, often in ways largely unnoticed. Those firewalls and anti-virus systems protecting you from unsavory elements? Backed by AI algorithms. That smooth corporate Internet connection? Managed and load-balanced by sophisticated learning-based software. The energyefficient new office space? AI climate and lighting control. The great career boost you got when your company identified you as a "high potential"? AI helped you there too. On the home front, AI helps you shop, communicate, be entertained, and more.

Just about any area you look today uses AI and AI-enabled automation behind the scenes to accomplish a wide variety of operational and servicerelated tasks, without all the fanfare the media heaps on the Holy Trinity (Microsoft, Google, and Amazon). This "overnight revolution" has been more of a gradual transition, building over the years as cheap hardware, easier to use software, and skilled developers and data scientists all became more prevalent. Companies of increasingly modest means are now able to embed machine learning capabilities into key elements of their solution, and their customers benefit – without needing to invest millions building their own capabilities.

No corner of the corporate space these days is out of bounds. Companies providing solutions in HR, finance, customer support, sales and marketing, facilities, IT, even strategy and software development are increasingly using decision support and automation to improve outcomes for their customers. Microsoft, Salesforce, and Oracle are good examples of companies AI-enabling significant aspects of their existing product portfolio, which collectively reaches a large swath of companies.

Put another way: we've been so worried about AI taking over our jobs that we missed them becoming our co-workers. These algorithms sit by our side, nudging us in productive ways and even making many of the simpler decisions we used to make. And in the next few years, these capabilities will permeate even more areas of our work life.

We are becoming increasingly de-sensitized to the concept of AI and resetting our expectations accordingly. Not long ago, AI was mostly met with fear and confusion, complements of a media and entertainment industry that feeds on our fascination with doomsday scenarios. Recent warnings from tech luminaries helped fuel that fire. While a healthy fear still exists around superior general-purpose AI, an increasing number of people see narrow task-based AI as the utility it is rather than a threat. We are also starting to see computers as fallible, a significant shift from the mindset of the past few decades, where perfectly executing procedural machines were the expectation. These shifts have opened the door for people to be more comfortable with AI and automation. They are willing to work with the technology and understand its limitations. In the terms of Gartner's hype cycle, we have moved out of the "trough of disillusionment"and into the "plateau of productivity".

With this newfound comfort in AI technology comes the rise of citizen AI scientists. Like citizen data scientists, these hobbyists come from many walks of life and sit within different departments of the organization. While they might not be able to build a sophisticated new algorithm, they are adept at monitoring advances, championing the use of AI, and helping select, implement, and train capabilities. These advocates will further the spread the daily use of such technologies.

Finally, as AI and automation becomes more pervasive in our work and home lives, the way we interact with computers will transform. Even with advances in user experience and device interaction, we still spend most of our time with new technology learning how to use it. We conform to its expectations and rules. But as systems get smarter, increasingly they will adapt to us.

We won’t have to hunt for information, for example. In tomorrow’s world, it will be served up to us exactly when we need it.As AI becomes more commonplace, we will start to see the competitive landscape flatten, with most every company benefiting in the same way from advancements in smart machines and automation. Day-to-day operations will be improved for all, and competition will shift to the edges, with more advanced companies innovating AI into their core business models. The savvy organization will take the lessons they’ve learned from everyday AI and find ways to align that technology with their key drivers of growth.

Neha Kothari
BE IT

Cyber Security and your Business Impact Analysis, Understanding RPO and RTO in Disaster Recovery

While all businesses need to survive a disaster and the problems that follow, it’s nearly impossible to predict when a disaster will happen. Businesses will often push cyber and IT security out as an optional expense with an attitude of “if it ain’t broke don’t fix it.” When the disaster strikes (and odds are increasing at a fast pace for both natural disasters and cyber attacks), don’t leave your business unprepared. Planning will help you respond quickly.

An important aspect of your IT and Cyber Security plan is to work with your IT security provider to complete a business continuity plan that includes a complete business impact analysis (BIA). Often, this is the first step to identify critical system and components that are essential to your organizations success. Key questions during the BIA include:

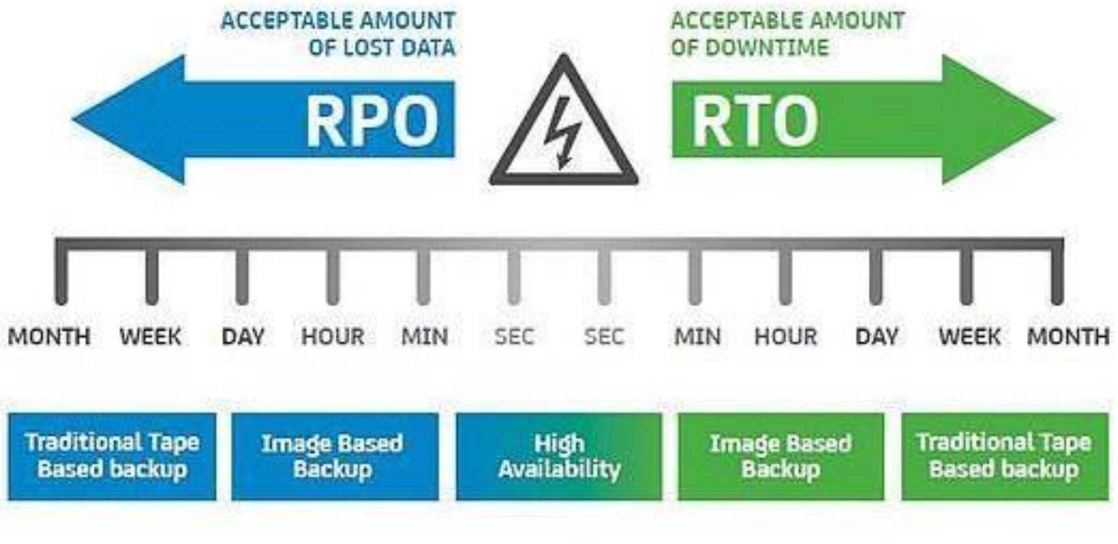
- What are your critical systems and functions
- What are the dependencies related to these critical systems and functions
- What is the maximum downtime limit of these critical systems and functions
- What scenarios are most likely to impact these critical systems and functions
- What is the potential loss from these scenarios

Walking through these questions will help you identify key processes and dependencies as part of your overall disaster recovery and business continuity planning. Each step of this plan must satisfy two measurements: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO and RTO are measured in specific time intervals or number of hours relating to the loss of data and service time.

How long can your business be without the service before you incur substantial loss?

RTO (Recovery Time Objective) can be defined as the start of the interruption and time to establish recovery and end when you can successfully release the service back to your users. The goal is to calculate how quickly you need to recover and then to map out the people, processes and budget allotment you will need towards business continuity.

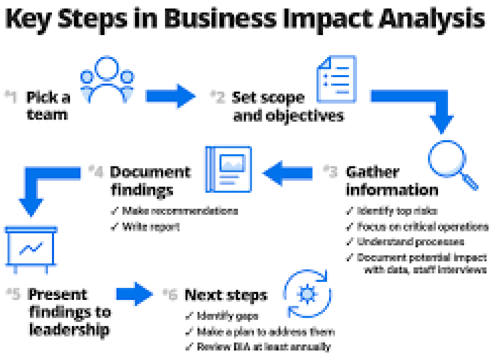
RPO (Recover Point Objective) often refers to the last available restore backup and the maximum time between backups being safely stored offsite. This focus is on your data and your company loss tolerance – how long can you afford to operate without your data before your business suffers.


ACCEPTABLE AMOUNT OF LOST DATA
RPO
ACCEPTABLE AMOUNT OF DOWNTIME
RTO
MONTH
WEEK
DAY
HOUR
MIN
SEC
SEC
MIN
HOUR
DAY
WEEK
MONTH
Traditional Tape Based backup
Image Based Backup
High Availability
Image Based Backup
Traditional Tape Based backup

Both RTO and RPO influence the type of redundancy and backup infrastructure you need to have in place. Besides time and money, you will need to consider compliance and your trust reputation with your clients.

Business Impact Analysis

Key takeaways from the business impact analysis should detail a listing of your critical systems and processes ranked by priority. This list should include 3rd party vendor software, cloud software usage, on premise software, on premise hardware that affects day to day operations (phone systems, devices used by employees, fax machines), IT infrastructure and even access and security to your property. As you walk through each system, you will record these items: • Potential impact scenarios • RPO including actual back up times • Dependencies • Likely impact • RTO • Potential loss Ranking all of your systems and infrastructure by priority will give you a clear map of what needs to be recovered first and what can possibly wait. Identify the manual process and the automated processes as well and include vendor contact information for assistance on each of these systems.


Key Steps in Business Impact Analysis
#1 Pick a team
#2 Set scope and objectives
#3 Gather information
✓ Identify top risks
✓ Focus on critical operations
✓ Understand processes
✓ Document potential impact with data, staff interviews
#4 Document findings
✓ Make recommendations
✓ Write report
#5 Present findings to leadership
#6 Next steps
✓ Identify gaps
✓ Make a plan to address them
✓ Review BIA at least annually

If you are subject to compliance regulations, protecting your data isn't optional, it is a legal obligation. Disasters happen, cyber warfare is real, and the best resolution is to detail and plan, assign priority duties and communication paths, practice and budget accordingly.

Gagandeep Singh & Dhanashri Mundada
BE IT

Autonomous Swarms: The Power of Group Robotics on the Blockchain

Flocks of birds, schools of fish, swarms of insects, and now... swarms of robots. Inspired by their biological counterparts, robot swarms comprise many individuals that together accomplish a task each individual robot alone cannot. Autonomous Swarms - the combination of swarm robotics and blockchain technology - is one of the 2019 emerging technology trends covered in Info-Tech's 2019 CIO Trend Report.

This year's report focuses on transformative combinations of technology. Robot swarms can exist without blockchain, but combining blockchain technology with swarm robotics pushes Autonomous Swarms past a critical threshold of security and reliability. This makes them suitable for deployment in many of the currently hypothetical use cases.

What are Autonomous Swarms?

Autonomous swarms combine the technology of swarm robotics with a blockchain-based back end. Not to be confused with collaborative robotics (several robots working together as an assembly line), swarm robotics involves multiple copies of the same robot, working independently in parallel to achieve a goal too large for any one robot to accomplish. The blockchain is a distributed ledger technology that creates an immutable, decentralized record of information. Storing information this way creates advantages such as auditability, trust, efficiency and security. By leveraging the benefits of both swarm robotics and blockchain, Autonomous Swarms has the potential to enter into new use cases - such as city cleanup, agriculture, traffic surveillance - where trust and information security are key challenges to automation.

KILOBOTS
A thousand-robot swarm uses collective artificial intelligence

Why use Autonomous Swarms?

As the business's technological steward, today's IT leader must help their organization adopt emerging technologies with an eye to their long-term impact, by focusing on both business and human benefits.

Business benefits of Autonomous Swarms:

- Scale - Every agent within a robotic swarm is designed to act autonomously, with the overall swarm behavior emerging organically as a consequence of these individual tasks. This makes it simple to increase or decrease swarm size simply by adding or removing agents.
- Decentralized Decision-Making - Blockchain technology allows multiple robotic agents to reach consensus without the need for a central authority through "voting". This makes the swarm more resilient and simplifies the job of a human controller.
- Consistent Results - The blockchain enables swarms to perform their jobs more robustly, with less potential for error and malicious interference. This leads to more consistent and dependable results for businesses.

Human benefits of Autonomous Swarms:

- Dangerous Situation Avoidance - Robot swarms are ideally suited to take over dangerous or undesirable jobs such as landmine detection, dangerous machinery maintenance and city cleanup, where automation can greatly improve the quality of life of human workers.
- Resistance to Hacking - In applications where robots are in close proximity to humans and their data, the resistance to malicious attacks afforded by blockchain means greater peace of mind for the people whose data robotic swarms may be handling.
- Error Avoidance - Consistency and dependability result from the decision-making and auditability possibilities blockchain opens for robotic swarms. For humans, this means less worry about errors in handling tasks such as pesticide use in crops.

Where is the technology now? A swarm robotics case study

In Australia, SwarmFarm Robotics is developing a farming approach using swarm robotics that is targeted rather than sweeping: using multiple autonomous machines, smaller than traditional farming machinery, to perform targeted actions, such as administering pesticides only where they are needed. Where the old approach was to take a large tractor, capable of spraying several rows of crops with pesticide simultaneously, the smaller robots use artificial intelligence to roam the field, identify weeds, and spray only them, leaving crops intact.

SwarmFarm’s robots have been adapted to other applications, including irrigation, planting, weeding and harvesting. In all cases, a more targeted approach means greater precision and economy of resources. Pesticide and fertilizer can be applied more sparingly, and planting and harvesting can be done with individual attention to each plant, an impossible task with large-scale machinery. The new approach produces greater yields at reduced cost, while raising the quality of the crop.

Several robots have been under development and testing on SwarmFarm land. SwarmFarm has garnered support through government funding, and partnered with PWC Australia, Adama Australia, Bosch and other sponsors to bring the robots to market.

Are Autonomous Swarms right for your business?

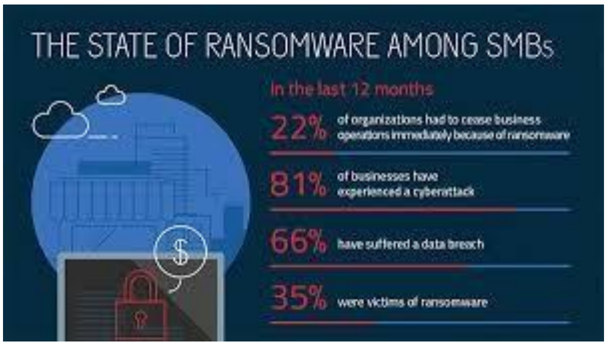
When evaluating whether this technology is worth investigating further, consider: do you have a use case? Autonomous Swarm robotics is a powerful solution primarily for problems that are amenable to a distributed approach. If you have such a use case, consider how the key dependencies will affect it. For example, data privacy may not be as important for farming as for city surveillance. If you are an IT leader looking to capitalize on Autonomous Swarms, identify the key dependencies specific to your industry and learn about the current cutting edge solutions.

ChinmayNanaware & Pushpak Khamakar
BE IT

Matrix and Emotet

When people talk about cyber attacks, they're often talking about widespread, common threats like phishing attacks deployed by low-skilled criminals. We've grown used to the idea of throngs of opportunistic cybercriminals sending out high-volume attacks, like email flooding, hoping that some might take root and score them a quick buck.

But as tools have been put in place to block those attacks, cybercriminals have evolved in turn. Targeted ransomware attacks are on the rise, with higher skilled cybercriminals carefully selecting targets to hack manually. And other malware attacks have grown more and more sophisticated, to keep evading security tools.



THE STATE OF RANSOMWARE AMONG SMBs

In the last 12 months

22% of organizations had to cease business operations immediately because of ransomware

81% of businesses have experienced a cyberattack

66% have suffered a data breach

35% were victims of ransomware

Recent threats like Matrix and Emotet demonstrate the various ways that cybercriminals have changed their tactics to stay effective and profitable in today's marketplace. We'll dig into what makes Matrix and Emotet unique and so dangerous, and what enterprises should be doing to protect against these and other similar threats.

Matrix: The Niche Targeted Ransomware

With many advanced cyber threats, usually "who you are" is what makes you a target. With targeted ransomware like Matrix, though, the "what" is what makes you a target. Cybercriminals are looking for a vulnerability – things like unpatched web servers or an exposed Remote Desktop Protocol (RDP) host – and if you have one, you're a target.

Targeted ransomware takes advantage of exposed or vulnerable hosts on the internet to manually, deliberately hack into a system and deliver ransomware. What sets targeted ransomware apart from other threats is that it's manually implemented – there's a human making decisions and adapting to roadblocks along the way.

Attackers using Matrix, a niche targeted ransomware, are known to infiltrate a company’s network by brute forcing their way into exposed RDP hosts. Once inside the network, attackers will escalate their privileges to become an administrator or domain administrator, and use any number of techniques to deploy the ransomware, demanding ransoms around $3,500. The unfortunate truth is that many organizations still permit Windows computers with weak passwords to be exposed to the internet, creating a massive opportunity for targeted ransomware groups to exploit. That’s how Matrix has been able to cause damage and mayhem recently – by attacking that low-hanging RDP fruit.

Emotet: The Shape-Shifter

Compared to Matrix, Emotet is more of the opportunistic type of threat we’re used to seeing. This network worm is typically sent out with a “spray and pray” mentality, where cybercriminals send out large volumes of attacks and hope to infect as many people as possible. That’s vastly different from the slow, deliberate, manual approach that targeted ransomware takes.

Emotet is a great example of how a threat can evolve in order to stay relevant and maintain a revenue stream.

Since 2014, Emotet has evolved from primarily being a credential stealer and banking Trojan into a modular, polymorphic platform for distributing other kinds of malware. The worm has three main goals: spread onto as many machines as possible, send malicious emails to infect other organizations, and download a malware payload.

It’s also incredibly dangerous. The US Department of Homeland Security considers it one of the most costly and destructive threats to businesses today.

What makes Emotet so dangerous compared to many of the other opportunistic threats is its ability to change shape and spread without the aid of a user. That means that once it infects one computer in an organization, it can quickly spread across the entire network. And as it’s cleaned up, it has the ability to morph and re-infect the same machines.

To make matters worse, Emotet often also tries to turn a malware infection into a data breach by stealing email addresses, web histories, or even usernames and passwords. And we’ve also seen targeted ransomwares like BitPaymer use Emotet as a delivery mechanism.

How can enterprises defend themselves?

Sophisticated threats like Emotet and Matrix can be utterly devastating to infected organizations. Once a cybercriminal gains control over the network, there’s no limit to the damage they can inflict. The most important thing organizations can do to reduce the likelihood of becoming a target is build a strong security foundation to protect against all manner of attacks.

Think of it this way: Imagine a thief walking down the street at night in your neighborhood trying to open car doors. If a car door is locked, they’ll move on. But if they find one that’s unlocked, they’ll open the door and steal all the contents of the car. That’s what’s happening with these attacks. Enterprises need to be doing everything they can to lock the door, so to speak, and that starts with security fundamentals.

Patch your systems, especially those exposed to the internet. Take RDP machines and put them behind a VPN with two-factor authentication.

Beyond that, make sure you’re using all the best security tools at your disposal, like exploit prevention tools that provide protection from endpoint to firewall. Innovative technology like deep learning can help protect against a polymorphic threat like Emotet, with the ability to recognize and block new variants.

Here’s the bottom line: If your enterprise is connected to the internet, the risks may be both broader and deeper than you realize. It’s time to invest in innovative security software that’s easy and intuitive to use. For more information on Sophos security solutions visit www.securecontenttechnologies.com, for Emotet, Matrix and other cyber threats, go to Sophos.com

Vedant Ghavate
BE IT

Multifunction Printers and Copiers: IT Security

Over the last decade, office technology has advanced tremendously. Networked printers and copiers have taken this technology to the next level, providing businesses and organizations with a host of advantages such as flexibility, functionality, increased efficiency, and reduced costs.

Unfortunately, many organizations are not aware of the potential risks involved with networked printers and copiers. Like computers, today's networked multifunction printers and copiers are vulnerable to data breaches unless they are secured. A wide range of organizations, from schools to hospitals to businesses, are all putting themselves at risk with unsecured end-points running on their IT networks.

The purpose of this article is to provide you with an overview of the steps you need to take in securing your multifunction printers and copiers to protect your valuable data and sensitive information.

Performing an Audit of Networked Printers and Copiers

Depending on the size and scope of its operation, it is not uncommon for an organization to be unaware of what devices are connected to their network, or whether these devices have been configured with the proper security checks. The printers and copiers themselves can create a security risk if they are running with outdated firmware. An aspect of security that is often overlooked is once you are ready to retire a printer/copier or return it to a leasing agency, it is crucial that you remove any data that may be retained in the hardware's memory. Ensuring that the device's hard disk is erased, destroyed, or removed will provide you with a final added measure of security.

Securing Access

Start the process of defending your printers, documents and data from network threats by physically securing your printers and copiers. If possible, move printers that are out in the open into a controlled access area. Access can further be controlled by disabling physical ports to prevent unauthorized use. Data can also be protected by authenticating users and attaching them to their specific documents. Document owners are then required to authenticate themselves to the printer or copier before their documents will print.

Disabling Unnecessary Services and Protocols

To provide the users of office technology with efficient, turn-key product solutions, many printer and copier manufacturers are offering models with a wide range of services and protocols built in. Many of these enabled-by-default protocols are unnecessary and not secure. Leaving these services enabled may provide attackers with the ability to access the printer/copier data directly.

Securing Data with Encryption

Wireless technology has been an amazing advancement in promoting efficiency and productivity in the workplace. Unfortunately, with the benefits come risks. Your documents and data become highly vulnerable as they traverse the "wireless network" to a multifunction printer or copier. Once your information makes it to the hardware's memory or storage, it is susceptible to attack there as well. The best way to protect sensitive data within your network is with encryption. Encrypt print and copier jobs to secure data in transit in the event of interception and use encrypted storage to protect documents in the device’s queue.

Keeping Up with Patches and Updates

The importance of staying on top of software and hardware firmware updates cannot be overstated. This includes the firmware used in your multifunction printers and copiers. Some printers and copiers with an internet connection will automatically check for new firmware and install it. Others will require you to periodically to visit the manufacturer website for firmware update downloads, which you can retrieve and install yourself. Ignoring updates and patches will likely result in the development of critical vulnerability points in your network.

Selecting Secure Multifunctional Printers and Copiers

Without a doubt, the best way to secure your printer and copier is to invest in technology that is pre-programmed with the most up-to-date device security features. Look for multifunction printers and copiers that are designed to independently detect, protect, and self-repair damage from malware attacks. As you upgrade outdated equipment, replace it with systems that offer built-in threat detection and software validation features, so only authorized firmware and software can be installed and executed. This will provide your network with an extra layer of security.

Muskan Shaikh

TE IT

Company Email vs Personal Email – A Necessary Separation

As administrators, we sometimes must deal with as many user issues as we do technology issues. One of those issues is email. We may have employed great spam and phishing solutions, yet the users still receive that occasional email that makes it through our filters and causes issues.

Surely you have heard the story of the employee who bought a stack of iTunes gift cards for the "CEO" and sent the codes to the phisher. Despite our best protections, people are always going to find a way to get through. One of the best things you can do to minimize the amount of exposure your company gets is to require that employees use their company email address for company business only.

There's usually only one argument for using company email for your personal email: it is convenient. That is a weak argument considering the significant consequences that could cause.

If you use your company's email for personal use, consider the following:

1. Your personal email is archived per the company's standards. This could be potentially forever and subject to eDiscovery searches and disclosures. If you don't want your personal email to end up in a court filing, don't use the company's email.

2. Your personal email should be private. Corporate email is not private. Administrators and other company officials must have access to your unencrypted email in order to provide necessary services.

3. It increases the amount of SPAM the company receives. By posting or registering with your company email address in forums and services, it gets on more and more lists, and becomes involved in more breaches. Verified corporate email addresses are valuable to people doing spear phishing and blind marketing (also known as unsolicited commercial email.)
4. It increases attacks against the company and can lead to successful attacks.When a forum or online service is compromised, user and password

combinations found are used against other services. If a compromised user has a corporate email address, they'll immediately start trying that same password and derivatives against your corporate email account and other corporate assets. Password reuse is a big problem.

5. It increases the amount of email the company must save.
This increase in cost to the business can be significant. Storage costs are one thing, but backup costs, DR, archiving, eDiscovery searches, email migrations, and other efforts made harder by storing non-business email can significantly balloon the costs to the business.

6. Your email and your intellectual property are not your own. Read your company policies. You will likely find that anything created, stored, or processed on company equipment is owned by the company. This means that the idea you had for a startup that you emailed to a friend can be taken and used by the business whose email you used.

7. Job searching may be monitored. Some businesses pay attention to emails from job boards. If you don't want your boss to know you are hunting, use a different email address. Even if you are not job hunting, you may get these emails and cause concerns. When you do change companies, you have a lot of people to notify about your new email address, and you may lose emails sent to your old address.

8. Your email is only as safe as the company hosting it. If you are let go or the company goes out of business, your email may be gone forever. If the company has any IT infrastructure failures or breaches, your email may be lost or exposed to unknown hackers.

9. When you leave the company, even if you manage to take a copy of your personal email with you, a copy remains behind. It is common practice in many businesses to archive that email and make it available to your replacement(s). Deleting your email and emptying your trash is not enough since many businesses have backups or archiving that you can't delete. Many businesses consider the email you accumulate to be an asset and will recover it if you delete it upon leaving.

There are things businesses can do to facilitate this policy change and mitigate against employees who will not change. These include:

1. Make and publish a policy that clearly defines how corporate email is to be used. Enough said.

2. Allow access to email providers through your corporate web filter. There is a philosophy that says if you allow this your employees will waste too much time doing personal email. You, as an administrator, should always champion the idea that personnel problems should not be solved with technical solutions. If an employee is spending too much time checking their email instead of working, blocking their email won't suddenly make them a star employee. They will just find something else besides work to occupy their time. Personnel productivity problems should be solved with management and HR, not IT.

3. Enable credential reuse blocking. If your firewall (Palo Alto for example) provides this ability, it can prevent the reuse of your main credential on third-party sites, although it cannot stop every abuse.

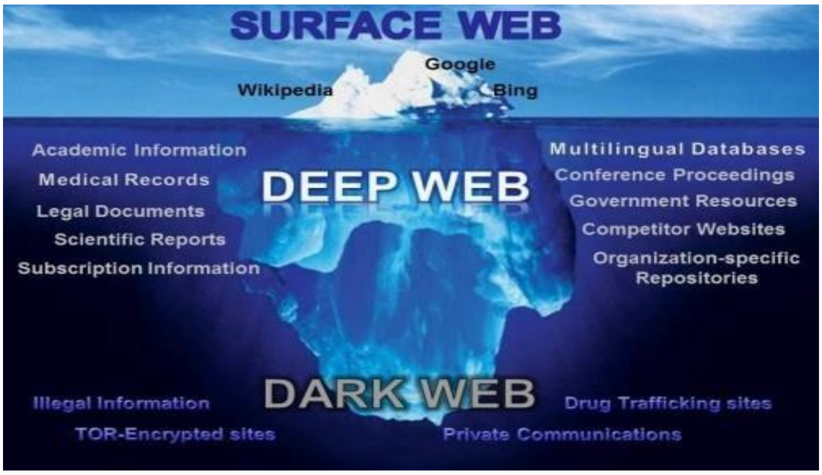
4. Extreme measures. After employing the above, you may have to actively block emails from domains that are clearly not related to your business.

5. Create additional email addresses. In some cases, it might be required for an employee to have a corporate email address that is given to a questionable site. Consider creating an additional email address or alias for those people so that messages received on that alias are clearly different.

RichaSirwani
TE IT

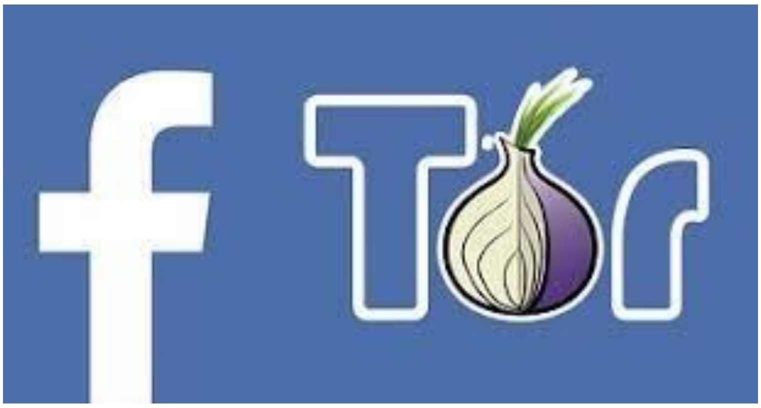
Dark Web

The dark web is a part of the internet that isn't indexed by search engines. You've no doubt heard talk of the "dark web" as a hotbed of criminal activity — and it is. Researchers Daniel Moore and Thomas Rid of King's College in London classified the contents of 2,723 live dark web sites over a five-week period a couple of years ago and found that 57 percent host illicitmaterial.

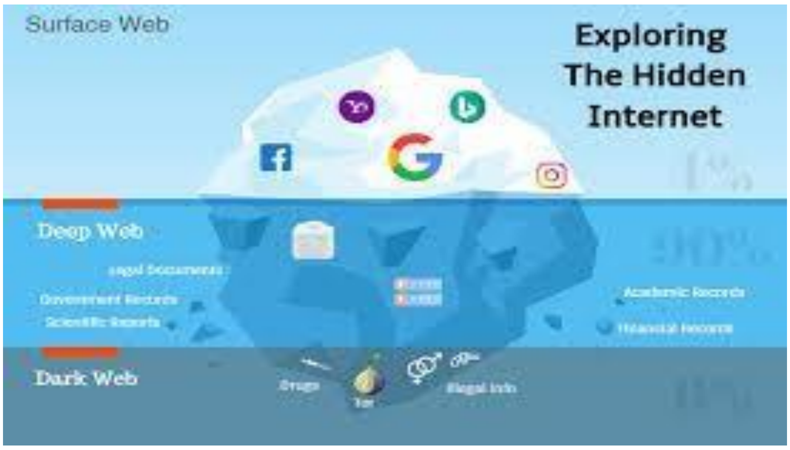


You can buy credit card numbers, all manner of drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers. Buy login credentials to a $50,000 Bank of America account for $500. Get $3,000 in counterfeit $20 bills for $600. Buy seven prepaid debit cards, each with a $2,500 balance, for $500 (express shipping included). A "lifetime" Netflix premium account goes for $6. You can hire hackers to attack computers for you. You can buy usernames andpasswords.

The place is as messy and chaotic as you would expect when everyone is anonymous, and a substantial minority are out to scam others. Accessing the dark web requires the use of an anonymizing browser called Tor. The Tor browser routes your web page requests through a series of proxy servers operated by thousands of volunteers around the globe, rendering your IP address unidentifiable and untraceable. Tor works like magic, but the result is an experience that's like the dark web itself: unpredictable, unreliable and maddeningly slow.



Dark web search engines exist, but even the best are challenged to keep up with the constantly shifting landscape. The experience is reminiscent of searching the web in the late 1990s. Even one of the best search engines, called Grams, returns results that are repetitive and often irrelevant to the query. Link lists like The Hidden Wiki are another option, but even indices also return a frustrating number of timed-out connections and 404 errors.Dark web sites look pretty much like any other site, but there are important differences. One is the naming structure. Instead of ending in .com or .co, dark web sites end in .onion. That's "a special-use top level domain suffix, designating an anonymous hidden service reachable via the Tor network," according to Wikipedia. Browsers with the appropriate proxy can reach these sites, but others can't.



Ritesh Chaudhary
TE IT

Seamless Connectivity

As more organizations make the shift to a hybrid IT infrastructure, data is increasingly dispersed across various networks, often in different geographical locations. As a hybrid IT strategy becomes the norm for organizations, executives and IT decision makers must ensure that public, private and hybrid solutions are accessible to every business, partner, end user and customer. So the question becomes, how do you maintain a cohesive IT strategy among different networks and environments? Enter interconnection. With seamless integration of your network infrastructures, organizations can ensure maximum uptime and complete IT availability for their business - no matter the data's location.

❖ Connect All of The Moving Parts

This is one of the most important aspects of transitioning to hybrid IT, but it is also one of the trickiest. Your infrastructure likely has many moving parts and applications that rely on multiple data sets found in disparate locations. To have a successful migration, you must keep in mind that data and applications are intrinsically linked. It is critical that you understand how much each application consumes and produces before simply picking it up and moving it. To do this, companies should consider storing manageable amounts of data in an on-premise location with hyperscalers, or with a data center provider, allowing each application to properly connect to the correct data store. This way, its unique needs are accommodated for and your organization will be set to achieve an efficient and ultimately successful migration process.

❖ Focus on the Long Term

When it comes to interconnection, it's not productive to get wrapped up in the "here and now." Always have the future of your workloads in mind. (Side note: This also rings true for enterprises looking to implement a disaster recovery plan or solution). It's critical to recognize your organization's plans to replicate IT processes with interconnection. You'll also need to carefully consider compliance, your company's downtime allowance and the most effective ways to store your most sensitive data. While the process can seem challenging and time-consuming, ensuring proper interconnection will, in-turn, allow you to put more time, energy and resources back into your organization. Keep your eye on the prize: a stable and secure IT environment.

- **Master Management and Monitoring**

Once a solid interconnection framework is established and your data is sitting in different locations, make sure you set aside time for it to adapt to its new environment. Once you’ve been able to work out the kinks, retaining agile workloads is key to the success of your interconnection strategy. Maintaining agile workloads goes hand-in-hand with creating opportunities for open communication among your peers and colleagues. Discuss the goals you would like to achieve with interconnection and institute a routine for consistent and effective monitoring. Without proper interconnection, you risk losing time, money and resources -- all of which make an organization’s IT operations thrive. By developing a more well-rounded, cohesive approach to planning and executing an interconnection strategy, you are making a smart business investment toward the long-term success of your organization’s most sensitive and critical data.

Ruchir Bhagwat
SE IT

Deep Learning

Deep learning (also known as deep structured learning or hierarchical learning) is part of a broader family of machine learning methods based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, semi-supervised or unsupervised. Deep learning architectures such as deep neural networks, deep belief networks and recurrent neural networks have been applied to fields including computer vision, speech recognition, natural language processing, audio recognition, social network filtering, machine translation, bioinformatics, drug design and board game programs, where they have produced results comparable to and in some cases superior to human experts.

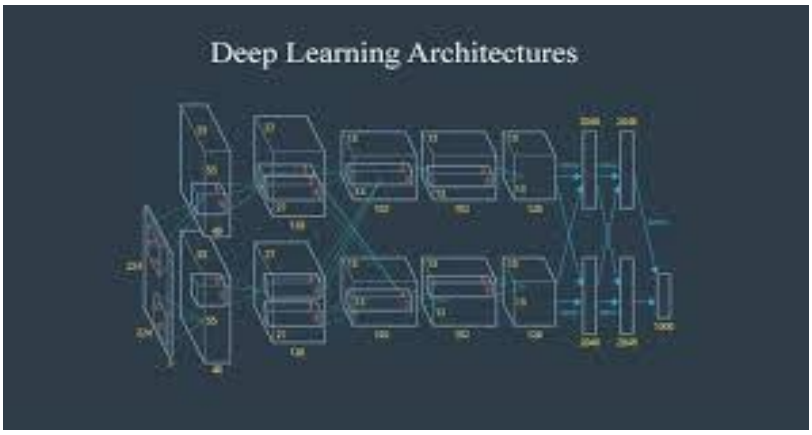
Deep learning models are vaguely inspired by information processing and communication patterns inbiological nervous systems yet have various differences from the structural and functional properties of biological brains (especially human brain), which make them incompatible with neuroscience evidences.

Most modern deep learning models are based onan artificial neural network, although they can also include propositional formulas or latent variables organized layer-wise indeep generative models such as the nodes in Deep Belief Networks and Deep Boltzmann Machines.

In deep learning, each level learns to transform its input data into a slightly more abstract and composite representation. In an image recognition application, the raw input may be a matrix of pixels; the first representational layer may abstract the pixels and encode edges; the second layer may compose and encode arrangements of edges; the third layer may encode a nose and eyes; and the fourth layer may recognize that the image contains a face. Importantly, a deep learning process can learn which features to optimally place in which level *on its own*.

The "deep" in "deep learning" refers to the number of layers through which the data is transformed. More precisely, deep learning systems have a substantial *credit assignment path* (CAP) depth. The CAP is the chain of transformations from input to output. CAPs describe potentially causal connections between input and output. For a feedforward neural network, the depth of the CAPs is that of the network and is the number of hidden layers plus one (as the output layer is also parameterized).

For recurrent neural networks, in which a signal may propagate through a layer more than once, the CAP depth is potentially unlimited. No universally agreed upon threshold of depth divides shallow learning from deep learning, but most researchers agree that deep learning involves CAP depth > 2. CAP of depth 2 has been shown to be a universal approximator in the sense that it can emulate any function. Beyond that more layers do not add to the function approximate ability of the network. The extra layers help in learning features.



Deep learning algorithms can be applied to unsupervised learning tasks. This is an important benefit because unlabelled data are more abundant than labelled data. Examples of deep structures that can be trained in an unsupervised manner are neural history compressors and deep belief networks.

Atharv Belurkar
SE IT

Future of Virtual Reality

As impressive and remarkable as the technology already is, many people believe it’s still in its early days. That’s because previous Virtual Reality-style efforts have been failure or flopped in the past (Nintendo’s Virtual Boy what has come to my mind). Anyway, the latest crops of gadgets are seen as even more promising, thanks to their much-improved abilities, graphics, and more.

The next evolution of Virtual Reality would be where you participate physically in that VR world indeed. And it’s not just about sitting down - if you’re a quarterback on example, you actually get to throw a football, and thus you can interface with the team. This is a kind of stuff that it’s going to happen. Headsets today are doing a great job at catering to your visual senses, and as well a little bit of audio. And that’s just 2 of the senses. Since you begin catering to the rest of the senses - temperature-wise, body-wise, and smell, the reality factor of VR becomes stronger and the virtual piece begins to fade.

Everyone rallied the PC gaming industry and now we have what we have today. VR is the same type of thing - no one company can solve all of the problems.There are so many people that don’t want to live a “normal” life. They deserve to be able to explore, live, and to experience the wonder of the world.The most obvious use for virtual reality is gaming! It offers an immersive, intense, and impressive experience that elevates gaming to practically, a whole new level.

The potential to fly around in space using a style interface similar to Google maps would be fun and interesting.Not so long in the future, VR would allow tours of museums for people that aren’t able to get to the building, also would let estate agents to give potential buyers a look around for the property without them having to leave the comfort of their own home.

Ankita Yekurke
SE IT