the BIT

JAN-JUNE 2017

the Bulletin of Information Technology

the BIT

-the Bulletin of Information Technology

ON CREATIVE DESK

Editors

PROF. KUTTYAMMA A.J
(HOD-Department of Information Technology)

MARY JOHN
Assistant Professor

ABEY ABRAHAM
Assistant Professor

Student Editor

ROSHINI KRISHNAN –S4 IT

Illustrations

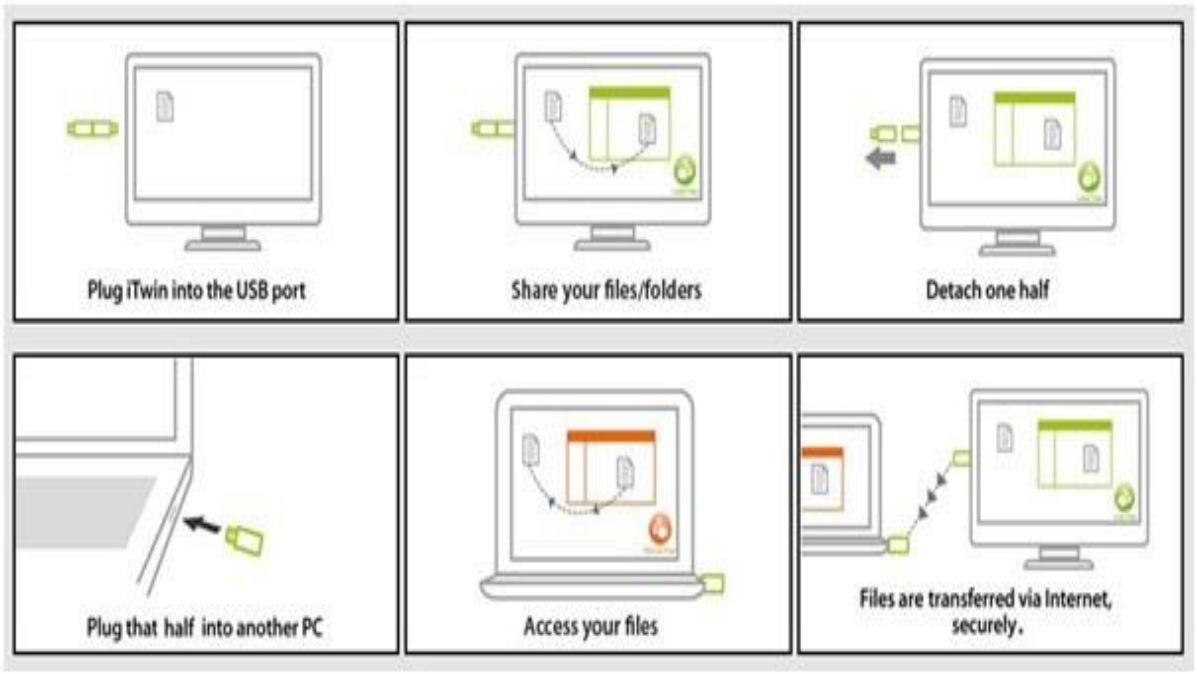
KRISHNADAS NADUVATH

CONTENTS

iTwin

iTwin is a revolutionary new file sharing and remote access device brought to you by a company called iTwin. It was invented by an Indian named Lux Anantharaman. 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 is a 'limitless' secure USB device that enables users to access, edit & share all their files & media between any two online computers anywhere in the world. The only limit is the size of your computer's hard drive. iTwin is an innovative solution that allows remote file access without the security and privacy risks of the cloud and USB flash drives. It's very easy to access as a USB device and no special installation is required. iTwin uses thoroughly analyzed crypto protocols and algorithms(AES 256 bit encryption). It has features like bi-directional file access, no temp files, remote disable, smart key generation, password support and twin trust authentication. It's so easy, it's unbelievable.



Working of iTwin

The iTwin Connect is a device similar to a USB flash drive but, is designed with two USB connections. The iTwin device is very dense and it establishes a secure connection between two computers or a secure connection between one computer and the iTwin server. When you connect the iTwin Connect device to the main computer in your home or at office, the software is automatically installed and configures the computer for remote connection.

When the device is disconnected from the main computer, you have to separate the two parts of .

the USB ports which are separated in two separate USB devices. The two separate devices are very dense at less than two inches. Small size makes it convenient and easy to carry with you all the time. When you connect the second half to your laptop while travelling on the road, it will routinely install itself without any user interference. In addition, you can set up a special password that disables the device if you are going to lose it. This ensures you can lock down your files to avoid access by an illegal user

Ms. Mary John

Asst.Professor

RANSOMWARE

Ransomware is a type of malicious software that carries out the cryptoviral extortion attack from cryptovirology that blocks access to data until a ransom is paid and displays a message requesting payment to unlock it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. The ransomware may also encrypt the computer's Master File Table (MFT) or the entire hard drive. Thus, ransomware is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key. Ransomware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file.

What is Wanna Decryptor?

Wanna Decryptor, also known as WannaCry or wcry, is a specific ransomware program that locks all the data on a computer system and leaves the user with only two files: instructions on what to do next and the Wanna Decryptor program itself.

When the software is opened it tells computer users that their files have been encryted, and gives them a few days to pay up, warning that their files will otherwise be deleted. It demands payment in Bitcoin, gives instructions on how to buy it, and provides a Bitcoin address to send it to. Most computer security companies have ransomware decryption tools that can bypass the software.

How to protect from ransomware

The cyber attack that wreaked havoc across the NHS over the weekend, leading to patients being turned away from A&E and some operations being cancelled, has continued to spread. The ransomware had targeted around 200,000 organisations in 150 countries.

The "WannaCry" ransomware appears to have used a flaw in Microsoft's software, discovered by the National Security Agency and leaked by hackers, to spread rapidly across networks locking away files. Ransomware is a kind of cyber attack that involves hackers taking control of a computer or mobile device and demanding payment. The attackers download malicious software onto a device and then use it to encrypt the victim's information. They threaten to block access to the files until a ransom is paid. It is common for criminals to ask for a fee between 0.3 and 1 Bitcoins (£400 - 1,375). Such attacks are mostly waged against businesses, but can also affect individuals.

Here are some ways to protect from ransomware:

Back up your files

The greatest damage people suffer from a ransomware attack is the loss of files, including pictures and documents. The best protection against ransomware is to back up all of the information and files on your devices in a completely separate system. A good place to do this is on an external hard drive that isn't connected to the internet. This means that if you suffer an attack you won't lose any

information to the hackers. Businesses often save copies of their data to external servers that won't be affected if their main network is attacked.

Be suspicious of emails, websites and apps

For ransomware to work hackers need to download malicious software onto a victims computer. This is then used to launch the attack and encrypt files. The most common ways for the software to be installed on a victim's device is through phishing emails, malicious adverts on websites, and questionable apps and programs. People should always exercise caution when opening unsolicited emails or visiting websites they are unfamiliar with. Never download an app that hasn't been verified by an official store, and read reviews before installing programs.

Use an antivirus program

An age-old computer security tip, antivirus programs can stop ransomware from being downloaded onto computers and can find it when it is. Most antivirus programs can scan files to see if they might contain ransomware before downloading them. They can block secret installations from malicious adverts when you're browsing the web, and look for malware that may already be on a computer or device.

Always install updates

Companies often release software updates to fix vulnerabilities that can be exploited to install ransomware. It is therefore advisable to always download the newest version of a software as soon as it is available.

Never pay the ransom

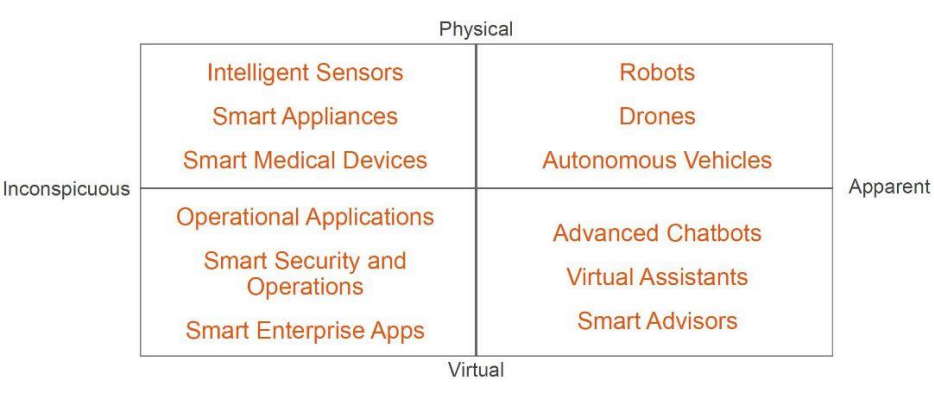
Victims of ransomware attacks are advised to never pay the fee as it encourages attackers and may not result in files being recovered. There are some programs that can help decrypt files. Or, if you have a back up, you can restore your device from that.

Jilsha James

MTech –S2 NE

An Era of Intelligent Apps

The future may be a collision between big data and application development that will yield a world of "intelligent apps". These "intelligent apps" combine customer, product and operational insights modern application development tools and user-centric design to create a more compelling, more prescriptive user experience. These intelligent apps not only know how to support or enable key user decisions, but they continually learn from the user interactions to become even more relevant and valuable to those users.



Intelligent apps, which include technologies like virtual personal assistants (VPAs), have the potential to transform the workplace by making everyday tasks easier (prioritizing emails) and its users more effective (highlighting important content and interactions). However, intelligent apps are not limited to new digital assistants – every existing software category from security tooling to enterprise applications such as marketing or ERP will be infused with AI enabled capabilities. Using AI, technology providers will focus on three areas - advanced analytics, AI-powered and increasingly autonomous business processes and AI-powered immersive, conversational and continuous interfaces. Gartner expects most of the world's largest 200 companies to exploit intelligent apps and utilize the full toolkit of big data and analytics tools to refine their offers and improve customer experience.

Adaptive Intelligent Apps are uniquely powered by enormous amounts of digital consumer and business data from Oracle's Data Cloud, sophisticated decision science/machine learning, and a scalable cloud infrastructure. They are data and context driven, continuously adaptive, self learning and action oriented.

Divyasree T H

MTech –S2 NE

LATEST TRENDS IN INFORMATION TECHNOLOGY

The information technology industry is always changing. New technology languages, architectures and platforms are introduced on a regular basis, as our world becomes more and more digitally connected.

There is also a growing demand for experienced IT professionals, as more businesses become increasingly digitized. The IT industry is growing faster than nearly any other field.

Our lives are becoming increasingly connected to our devices, other people and a variety of things. Smart machines get smarter, and a new IT reality must evolve with technology architectures and platforms to support the advancement of a digitally connected world.

Strategic

Trend 1: Disappearing Data Centers

More compute power will have been sold by infrastructure as a service (IaaS) and platform as a service (PaaS) cloud providers than sold and deployed into enterprise data centers. Most enterprises — unless very small — will continue to have an on-premises (or hosted) data center capability. However, with most compute power moving to IaaS providers, enterprises and vendors need to focus on managing and leveraging the hybrid combination of on-premises, off-premises, cloud and non cloud architectures.

Trend 2: Interconnect Fabrics

Data center interconnection fabric is poised to deliver on the promise of the data center as software-defined, dynamic and distributed. The ability to monitor, manage and distribute workloads dynamically, or to rapidly provision LAN and WAN services through an API, opens up a range of possibilities.

Trend 3: Containers, Microservices and Application Streams

Containers (e.g. Docker) and microservices are the new application platform for cloud development. Containers provide a convenient way to implement per-process isolation, which makes them well-suited for development of microservices, in which applications are constructed as a suite of small services that run as separate processes and communicate through lightweight network-based mechanisms. Microservices can be deployed and managed independently, and once implemented inside of containers, they have little direct interaction with the underlying OS.

Tactical

Trend 4: Business-Driven IT

Recent Gartner surveys have shown that up to 29 percent of IT spend comes from business units rather than traditional IT, and this will increase over the next few years. This business-driven IT was often a means of getting around traditional slow-paced IT processes. However, in today's world it is more often designed to provide technically savvy business people a means of implementing new ideas quickly, while adapting to, or entering, new markets as effortlessly as possible.

Astute IT leaders today recognize that business-driven IT has a real value to the enterprise, and that IT's role should be to build relationships with key business stakeholders –

thereby keeping central IT aware of new projects, and what their potential long term impacts will be on overall operations.

Trend 5: Data Center as a Service

IT leaders need to create a data center as a service (DCaaS) model, where the role of IT and the data center is to deliver the right service, at the right pace, from the right provider, at the right price. IT becomes a broker of services.

IT leaders can enable the use of cloud services across the business, but with a focus on picking the right service, at the right time, from the right provider, and in such a way that underlying IT service and support does not get compromised.

Trend 6: Stranded Capacity

Stranded capacity – things that are paid for, but not really used – can be found both in on-premise data centers and in the cloud. IT leaders should learn to focus not just on uptime and availability, but also on capacity, utilization and density. Fixing this can extend the life of an existing data center and reduce operating expenditures from providers.

Trend 7: IoT

The Internet of Things (IoT) will change how future data centers are designed and managed and how they evolve as massive volumes of devices stream data, constantly or periodically, to enterprises, government departments and agencies around the world. I&O should use an IoT architect who looks at the long term strategy for both IoT and the data center.

Organizational

Trend 8: Remote Device (Thing) Management

A growing trend for many organizations with remote sites/offices is the need to manage remote assets centrally. This has taken on more importance as enterprises focus on micro-data center support for regional or remote sites, and the emerging role of edge computing environments for geo-specific compute requirements such as the IoT.

The rapid adoption of IoT solutions by business units has introduced a new type of asset – connect sensors. The sensor may need to have firmware updates, or periodic battery replacement, which would require a new level of detail and control within an asset tracking and management system.

Trend 9: Micro and Edge Computing Environments

Micro and edge computing executes real-time applications that require high-speed response at the nearer edge servers. The communication delay is shortened to a few milliseconds, rather than several hundred milliseconds. It offloads some of the computation-intensive processing on the user's device to edge servers and makes application processing less dependent on the device's capability.

Trend 10: New Roles in IT

As IT evolves to adopt these trends, some new positions will be required within the ranks of infrastructure and operations. First and foremost will be the IT cloud broker, responsible for monitoring/management of multiple cloud service providers.

Next will be the IoT architect, tasked with understanding the potential impact of multiple IoT systems on data centers. This architect will also be working with business units to insure their closed loop IoT solutions are either

compatible with the central IoT architecture or that common protocols and data structures are used.

There will also be the need for an integration expert which may evolve into an integration team, responsible for insuring integration of new initiatives .

Sara Anil
S4 IT

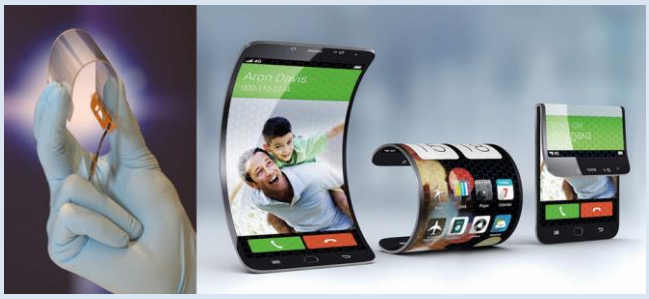
FOLDABLE TOUCHSCREEN AND SENSOR SKIN

A new inexpensive sensor was developed at the University of British Columbia which can help create such advanced devices a reality .The same technology can be used for making artificial skin that can sense stimuli and our body's vital signs.

The type of sensor was made by sandwiching a layer of highly conductive gel between two layers of silicone. It can sense different types of touches like swipe and tap (even when it is folded or stretched).

The prototype that was discussed in Science Daily measures 5cm x 5cm ,but can be scaled up because it uses inexpensive and widely available materials.

The same material can be used to cover anything that requires a transparent and stretchable touch screen. It is even possible to make room sized versions of this and put sensors on walls, floors or even on the surface of body and because this technology is cheap, it can be embedded in disposable wearables like health monitors.



Another major application includes, integrating the 'sensor skin' on robots and making human-robot interactions safer. If a robot could sense human presence and make its functioning softer, there would be lesser damage and exchanging tools with them would be easier. Now, machines are kept separate from humans in the possibility that they could injure humans. If this technology is brought into practice, then robots would be able to pick tools without damaging them and they can safely probe the environment.

-Reshma Mathai

S4 IT

Windows Nano Server:

Windows Nano Server is suitable for managing a cloud-based, 64-bit application that doesn't require any local real estate. With this low-maintenance Infrastructure-as-a-Service (IaaS) installation option, we can remotely control app's operating system (OS) without the security, capacity, and performance headaches associated with a full version of Windows Server. Let us see what Windows Nano Server is and how it's different from Windows Server.

What Is Windows Nano Server?

Unlike Windows Server, which is designed to manage local and cloud-based apps, Windows Nano Server is designed strictly for cloud operating systems (OSes) and apps that are developed directly on the cloud. Although we have access to full Windows Server driver support as well as malware protection, the apps are run entirely on Microsoft's cloud, without ever linking back to a physical server. This means it is running a faster, leaner, more basic server that's designed to avoid some of the struggles associated with larger server installations, especially update headaches and a larger security attack surface.

Let's break down the ways in which the business benefits from choosing the 64-bit Windows Nano Server. If not using Windows Nano Server for the following instances—as a compute host for Hyper-V virtual machines (VMs), as a storage host for Scale-Out File Server, as a domain name system (DNS) server, as a web server running Internet Information Services (IIS), or as a host for apps that are developed using cloud app patterns—one should probably opt for a more traditional server install.

Fewer Reboots

With Windows Nano Server, there is a dramatic reduction in the amount of times of reboot, which means it is more operational and much less annoyed.

Smaller Server Images

Large images take a long time to install, they clog up precious network bandwidth, and you'll quickly run out of capacity saving backup versions. The smaller Windows Nano Server images are quick to install, they transfer quickly, and they don't take up much disk space at all—all of which translates to consistent operations and more revenue.

More Room for Other Things

Use of less space on the server deployment, there is an increase of ability to store and transfer more data for other aspects of business. For example, more backups can be saved in the event of a disaster, or

additional corporate data can be stored which might have to be scrapped because of capacity concerns.

Better Security

Fewer moving parts in the server architecture means fewer access points for attackers. Because Windows Nano Server is a small, basic, and cloud-based utility, there are fewer entry points for attack.

Better Overall Performance

We should consider: random access memory (RAM) consumption. Larger server deployments eat up more of your computing resources, which ultimately slows down the performance of third-party apps. In order to ensure all of your apps are running optimally, a smaller server instance is ideal.

Roshini Krishnan

S4 IT