### Clouds Services and Servers

Cloud computing is the delivery (or offering) of various computing services i.e. Databases, servers, storage, networking, and software over the internet.

Cloud computing has been a buzz word for a few years now, many organizations and individuals have transitioned their traditional services into the “cloud”. The first advantage of using cloud services that comes to mind is the flexibility and scalability of resources. Secondly, with cloud services, you only pay for what you use, so immediate savings can bee seen. You don’t have to build your own data centre and fill it with your own infrastructure.

Most companies are simply not in a position to go out and purchase land, build a data centre, purchase infrastructure, hire people to configure and install the aforementioned equipment. Then, after everything is up and running, they will need to man the data centre and sustain the infrastructure. By utilizing cloud services, they simply rent to access anything from a few applications terabytes of storage from a cloud service provider.

Apart from large companies, individual users are also able to rent cloud services. People and companies can rent simple storage solutions, networking and virtual computers through to high end processing power and massive storage that will run artificial intelligence platforms. Another advantage of cloud services are you are able to run any application or service that you don’t need to be physically co-located with. Your cloud services may be physically located in Belgium, and you may be located in Dubbo NSW.

As technology advances, network transmission speeds increase and that is being passed on by network service providers. Unless you’re in Australia where the National Broadband Network (NBN) has not kept up standard or speed with the rest of the world. Large businesses that are transferring and processing large amounts of data cannot afford to be left behind and they need to adopt the evolving technologies to stay ahead of the competitors. Cisco are offering up 400gb speeds on their Nexus 9000 series switches. With that amount of bandwidth, massive amounts of data can be moved around in a quick fashion.

Microsoft Office 365 is very popular cloud-based service that is available individuals through to large companies. Microsoft offer a web-based portal providing access to applications like Excel, Word, PowerPoint, OneNote, OneDrive and many others. For very little cost, people are able to use these applications without having to download the application to their machine, all of the information is saved offsite (providing redundancy) and allows the user to access their data from anywhere in the world.

With the ever-increasing demand for cloud services, vendors had to come up with a solution to address emerging latency and bandwidth issues. One solution was to offload some processing tasks done by the CPU and pass that to the network infrastructure. An example is: In the Data centre environment the Network interface Card needs to a SmartNIC, passing some processing tasks that would usually be completed by the CPU. SmartNICs can perform network-intensive functions such as encryption/decryption, firewall, TCP/IP, and HTTP processing.

To increase the speed and efficiency of the data centers, more and more sharing of resources will need to occur. Utilising SmartNICs, servers running Graphics Processing Units (to provide resources to virtual machines). There will be further progression in the structured cabling space too. Having the fastest processor, with the fastest Network Interface Card is very useless if the data is only running over standard Cat5e copper cabling. Data centre structure cabling provides connections between devices utilising Optic Fibre. With advances in this infrastructure space, we will see faster transfer speeds resulting in higher bandwidth. NICs with a higher bandwidth capacity will be a flow on of higher transfer speeds.

With more and more people wanting to access and utilise cloud services, there will be a greater requirement for edge or access layer network architecture. These edge nodes or some people are calling them mini data centres will be required to assist in processes the additional data. They will need to synch up with their central data centre and more than likely need to be interconnected with one another. There will be increased employment opportunities for many industries:

• People that specialise in optic fibre installation.

• Builders required for building new data centres or refurbish existing building to be re-fit as data centres.

• Electricians, there will be a massive increase in power demands for a data centre. So not only data centre electricians, but substations will need to be taken into consideration.

• Air Conditioners installers. Data centres require a large amount of cooling in order to keep the infrastructure at the desired operating temperature.

• Network Engineers. The basis of any data centre is a good network. These engineers will be required for ongoing sustainment too.

• Virtual Machine/server engineers. Thick client desktops are slowly becoming a thing of the past.

• Project Managers. Depending on the size of the data centre, there will be a need for a project management team to facilitate the install and sustainment.

An increase in Data Centres across the world will have a large impact on the environment. Care must be taken to minimise any short or long term damage to the environment. Using recycled building materials, the installation of solar panels, planting of additional trees, and recycled filtered water for system cooling are all examples that will help to minimise the impact on the environment. With the installation of more cloud services, there will be an impact on other parts of the IT industry. There will be less demand for desktop engineers. Users will be utilising either Thin clients or something on a BYOD platform.

Up until about a year ago, I was a strong advocate for applications installed on my PC or Laptop. Not utilising cloud based much at all. I worked in an environment where security was paramount and traditional cloud services (Amazon, Office 365) were not an option. It wasn’t a foreign concept to me, it simply didn’t get exposed to the mainstream cloud services (like Office 365) in my personal life. Another consideration I had was security. I only had the one machine, I knew that machine was secure. If anyone had accessed my information, it was both my fault and my problem. So, I kept all of my data local, backed up with redundancy.

Within the last year, I changed employers, security was less of a focus and they utilised Office 365. Due to a change of personal circumstances, I found myself travelling most weekends to visit family. There were plenty of occasions where I wanted to access a document that I thought was residing my laptop, but in fact it was sitting on my PC located 2 hours away in the “My Documents” folder. I initially used to email various documents to myself, however I was having version control issues. I was losing track of when I updated the document and if it was the latest version. I also started at my new workplace, that would throw in another computer to “lose” files on. Where was the latest version of that file I was after? Work, home or laptop. Enter Microsoft’s “One Drive” cloud storage solution.

“Automatic backup for your Desktop, Documents, and Pictures folders

Saving files to the cloud is now effortless. Just set up PC folder backup for any of the three PC folders and OneDrive will do the rest by automatically syncing any changes made or new files added to your backed up folders.” - https://onedrive.live.com/about/pc-folder-backup/

The cloud service is free for users that only require less than 5GB of storage. Whilst it marketed as an automatic backup solution, I tend to not use OneDrive for that use. I simply use it as a Cloud Storage ‘my documents” folder. That solves my access issues as well as my version control problem.

Almost 2 years ago I separated from my wife and as a result my 3 children aged 15 13 and 9 relocated around 2 hours drive from me. Whilst I only see my children every second weekend, my 2 older children and myself use Snapchat to keep in touch. Snapchat is a multimedia mobile app that allows my children and I to send videos, pictures to one another. My eldest daughter is by far the biggest user of Snapchat, she has daily correspondence with hundreds of her friends. The advantage for my daughter using Snapchat Cloud service is, that the images are not stored locally. She sends hundreds of pictures a day on Snapchat, most are photos of nothing (please don’t ask, it’s a teenager Snapchat thing), if she was required to take a photo and then send it, she would have to go through her phone daily and purge the unwanted photos.

With Technology moving forward, bandwidth increasing and with more Data centres being built there will be an increased availability of types of services. As my children and I use mobile phones for the Snapchat application, I am hoping with advancing technologies there will be better coverage. With better coverage I believe there will be greater bandwidth to communicate easier and faster. Being able to communicate all the time, no matter where we are is very important to us, as we do not live together.

### Cybersecurity

#### What does it do?

Cyber security is an all-encompassing topic that over the last 10 years has become more and more prevalent in the public eye, but still retains an aspect of mystery as we transition into the age of information and technology. To give a brief overview of topic that cyber security covers, one need only make a brief list to begin to see the scope of the topic; Network security, Application Security, Identity management, database security, mobile security to name a few. However, the nature of cybersecurity is simple. To protect the integrity of networks, programs and ultimately sensitive data from damage or illegal access.

One of the most prevalent and upcoming technology for cyber security revolves around deep learning. The concept of deep learning is broader than just in regards to Cybersecurity, but essentially it’s the combination of machine learning and artificial intelligence to identify patterns through a type of deductive reasoning that uses contextual clues to indicate what is happening, this is based off and similar to the way human brains work. A current and widely used application for deep learning is image detection where each of the layers detects a pattern in an image that it has learned from previous images.

Two significant areas of cybersecurity that are greatly improved by deep learning is malware detection, and network intrusion. This is because systems like malware detection are currently heavily based on rule-based detection methods to deal with known threats. This leaves easily exploited holes in security due to the ability for attackers to simply tweak the malware signature to evade any current detection system. A significant benefit of this type of malware detection is that it can be applied to all types of platform including computers, smart devices and mobile phones.

By utilizing deep learning, we are able to treat malware programs like images, and apply deep learning techniques on these images to classify them as either malware or safe, this allows us to draw from commonalities in malware and to detect threats that may not fulfill all the rules of a traditional detection method.

With this being said, whilst an important aspect of cyber security is software, a lot of personal security relies on user generated passwords and protection, and it is eminently evident through repeated security breaches of people’s personal data that these methods are not adequate, as users have a tendency to use weak, easily identifiable passwords that can be breached with little to no effort for professional hacking individuals or groups. This has sparked a resurgence in hardware and multifactor authentication to add a further and less user-reliant form of protection.

Hardware authentication is both traditional, and new in many ways. It has been used by banks for a long time in the form of ATM cards, and some banks have used security tokens also, but is now more than ever accessible with the use of personal mobile devices as a secondary point of security. Companies like Google and Apple are now relying on user generated passwords, and a secondary point of verification usually in the form the user’s personal mobile device.

The impact of both of these technologies is profound on both a professional and personal level. For business’ deep learning technology is becoming near essential as we move towards a total reliance on technologically integrating business practices into the IT space. However, this progression also means significant risks, potentially crippling business’ if there are breaches to systems, which means lost revenue, and lost revenue depending on the impact can break business’ who are on the precipice.

Though the positives of deep learning cannot be stated enough, it also carries the risk of reduced jobs. As current malware and detection requires manual engineering that is consistently tweaked by software engineers. Removing the manual element allows more sophisticated and faster paced adaption to threats, but also may remove jobs that are currently essential to business’.

With regards to business’ and two factor authentication, it is common practice for major organisations to utilise key generating software and apps like authy in addition to passwords to add a secondary layer of protection for their networks. However, we may see in the near future a more biometric focused type of two factor authentication for business’ and or a wider adoption of hardware authentication in the form of keys.

On a more personal level, we may begin to see companies utilise their enormous data troves to create extremely sophisticated deep learning networks and integrate them with all future personal devices. However, in the near future, and currently we will be more impacted by the use 2 factor, and hardware authentication on more and more platforms. Companies like Mozilla and Apple are beginning to require two factor authentication for all add-on developers, and more and more companies are making 2FA a requirement, in fact google has launched an advanced protection program which utilises hardware keys that requires you to use these keys every time you want to log in to your account.

References

<https://digitalguardian.com/blog/what-cyber-security>

<https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security>

<https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field>

<https://www.analyticsvidhya.com/blog/2018/07/using-power-deep-learning-cyber-security/>

**https://towardsdatascience.com/malware-detection-using-deep-learning-6c95dd235432**

**Autonomous Vehicles**

The current state of Autonomous Vehicles as a whole is, frankly, an absolutely huge subject.

The simplest and most core of the idea is that a vehicle can, with the assistance of an onboard computer and sophisticated sensor technology, act in accordance with its surroundings to take action without the direct input of a human driver.

The general classification of autonomous vehicles comes under a five tier system, with each tier having specifics of what the vehicle can do, from simple driver assistance tools all the way up to fully automated trips between places without the need for human intervention.

In depth discussion of the technology is easiest with a knowledge of these tiers, which are laid out below.

#### **Tier 1**

Driver assistance technology is the most common and longest existing of autonomous vehicles, and some of these technologies have been around since as early as the 1950s.

These are relatively simple technologies such as cruise control, anti-lock brake systems (ABS) and stability control. These are all systems that will add convenience to a driver’s commute and safety while still requiring a human to stay in complete control of the vehicle.

#### **Tier 2**

The second tier of vehicle autonomy is the limited automation of one feature at a time in limited circumstances. Some variations of this technology have been around since around 2000 and the most well known of these technologies is automatic emergency braking, which will use sensors in the front of the car to automatically slow or stop the car when an obstacle is sensed in front of the car, such as a slower vehicle in the lane in front, a stationary obstacle sitting in the road, or in some cases an animal or person moving into the path of the vehicle.

#### **Tier 3**

Tier 3 is the highest version of autonomous vehicle technology that is available to the general public, with several large car manufacturers currently developing and improving their current offerings. Tier 3 allows for the onboard computer handling two or more simultaneous functions driving the vehicle, such as cruise control, automatic braking, and lane keeping.

Vehicles with this level of technology are able to maintain current actions, such as following a lane, sticking at a specific speed, and potentially avoid low speed collisions, but still require an active driver in control of the vehicle. Many of the vehicles of this level have driver monitoring implemented, so that if the driver is not paying appropriate attention to the operation of the vehicle, it will slow and move itself off the road to prevent potential accidents that the computer cannot handle by itself.

#### **Tier 4**

Tier 4 automation technology is still largely in development. It is able to largely take control of the vehicle, take full control of entire trips, and importantly does not require continual oversight from a human driver. A vehicle with Tier 4 automation is mostly able to handle emergencies and changes of circumstances, especially when in a controlled environment, but will notify the driver if and when anything occurs that it is not able to take care of by itself. With a vehicle of this type the driver would be free to undertake other tasks while being driven but should be awake and ready to take control if it is required.

#### **Tier 5**

Tier 5 automation, simply put, is complete and total automation of the vehicle. A tier 5 automated vehicle would be able to take any and all actions required to undertake travel completely alone without any input from a human whatsoever.

As stated above, tiers 3 and 4 are the most heavily under development at this time, with tier 3 being available to the public and being improved and refined while in use, and Tier 4 being actively under development but only available for use under strictly controlled circumstances.

Generally they use a combination of a number of different sensors including RADAR, LIDAR, and ultrasonic sensors to be able to tell what is going on around them, and utilise machine learning to improve and adapt based on what actions have been taken in similar circumstances previously.

A very large amount of the improvements in the quality of vehicle automation in the near future is going to come from machine learning, with Tesla making great strides in this department as they currently have the largest user base with all of their current model vehicles having their Autopilot installed as a standard. Machine learning takes cases where either an onboard computer tries something new, or records what the human driver’s intervention is, and records it for future use so that it can improve its reactions in future. It then will send the information back to the manufacturer where it is propagated across the entire range of vehicles, often on a per-manufacturer basis.

As an addition to this, there is a small number of firms working on a technology called “Vehicle to Everything communication” or V2X, which extends the idea of vehicles talking to each other, and adds traffic lights, weather services and other road services to the mix, allowing the vehicle to know more easily in real time what is happening around it, including traffic and road conditions, and with enough autonomous vehicles on the road, nearly eliminate the incidence of traffic accidents.

There are many potential impacts of wider improvement and implementation of autonomous vehicle technology, across several different industries.

To taxis in the short term it will make the driver’s job a lot easier, with the ability to simply input a destination and watch to make sure nothing happens. Unfortunately as the quality of the automation progresses, the drivers themselves will become less and less necessary, eventually reaching a point where an entire fleet will be controlled from the head office with no need for human oversight.

Similar could be said for the Trucking industry, with a huge pool of jobs that will be made simpler and less tiring on long drives in the short term, with there already being speculation that the local driver providing input in case of an emergency could be replaced by a remote driver overseeing large numbers of trucks and monitoring them for the need for human input.

Potentially the biggest industry these improvements will have an effect on will be the IT industry.

There is already a very large number of projects that are utilising machine learning and rudimentary AI in their technological research, and with the sheer size and scope of work being done on autonomous vehicles, the improvements in machine learning could be a driving force (pardon the pun) towards huge improvements across the board for software that will learn and adapt from previous experiences. Improvements in machine learning software for cars can potentially lead to improvements in a wide array of uses such as virtual personal assistants, email and spam filtering, and a whole variety of other applications.

On a more personal level, improvements in self-driving vehicles will have a huge impact to me on both a personal and a professional level.

A vehicle that is able to travel autonomously would mean being able to focus on other tasks while travelling, either locally or over long distances, which would alleviate boredom, fatigue and time that could be spent in other ways while travelling. It would open up the ability for me to more regularly visit friends and family in other cities and states across the country without losing valuable study and work time to travel.

To some of my family members the biggest benefit would be similar; the ability to conduct business, communicate with clients and continue working while travelling to collect mail or visit clients would be invaluable.

### Cryptocurrencies

Blockchain and Cryptocurrencies are a fascinating development that is currently ongoing in the IT world. It changes the way products and services can be paid for online, and with new upcoming developments, in person as well. Historic examples of this magnitude include the internet, smartphones, cloud computing, and public-key cryptography.

Blockchains are an internet based record keeping technology most well known as the technology behind bitcoin. Blockchain i sa distributed, decentralised public ledger, that could be described as a chain of blocks holding digital information. These blocks are able to store all sorts of information, such as the date, time and value of a purchase, who is participating in a transaction using a digital signature, and unique identifiers for the blocks themselves, called a Hash.

Every single block’s hash is unique. Even if you make two separate transactions at the exact same time, of the same product from the same source for the same amount, the block’s hashes will be unique and different so they can be told apart.

Public-key cryptocurrency is based on the internet is used to make trades anonymously. The most important feature of these cryptocurrencies is that they are not controlled by any central authority; the decentralised nature of the blockchain makes cryptocurrencies immune to government control and interference. Cryptocurrencies can also be sent between two people using public and private keys to avoid the cost of major bank fees.

Bitcoin is “Mined” by computers around the world by processing transactions on the blockchain with distributed computing.

As of the time of writing, the current price of bitcoin is $11,756.65 in australian dollars, and increasing global uncertainties will likely push more investors into bitcoin as it becomes recognised as a store of value.

While Bitcoin mining can be mined on a smartphone, it’s not a worthwhile solution as it will use a lot of energy for a relatively low power device; most bitcoin mining is undertaken on desktop PCs and in a larger amount by specialised large servers.

The better use of a smartphone when it comes to cryptocurrencies is as storage for your Digital Wallet. These digital wallets are used with most cryptocurrencies as a way to store your money; these style wallets are used, among others, by Bitcoin, Ethereum, Ripple, Litecoin, and Bitcoin Cash.

The wallet stores the public and private “Keys” or addresses which can be used to send or receive the currency. With the private key it is possible to write in the public ledger, effectively spending the associated currency by assigning it to another person’s key. The public key is used as a receiving address, which people can use to sign their currency over into your wallet.

Cryptocurrency is currently illegal in a number of countries, including Algeria, Egypt, Morocco, Nepal and Pakistan, and the countries that have a Banking Ban are Saudi Arabia, Jordan, Iran, Bangladesh, India, China, and Cambodia. These banking bans are essentially the local reserve bank disallowing any banking organisations from accepting or trading in cryptocurrencies.

However as the development of bitcoin is decentralised it is a promising development for a more financially inclusive world.

The rise of cryptocurrency can potentially have a huge impact on the real estate industry as it currently relies on an inefficient loop between Attorneys, financial institutions, and real estate agents, which has the effect of making transactions slow and cumbersome. This ineffective loop stems from a lack of guarantees of trust between parties, which can escalate costs by as much as 10%.

Blockchain technology and the use of smart contracts can revolutionise this process while complying with legal requirements. The smart contract code will facilitate, verify and enforce the negotiation or performance of any agreement or transaction.

Of course these advancements, while they are able to massively expand access, still require massive changes to financial law; they need a legal framework that is responsive and will enable them to work, and there are a lot of regulators and innovators in the tech space that are working hard to address this needed change. A leader of this is the Financial Services Commission in Barbados, who have created a working group to consult on the creation of new financial regulations that can be applied to digital assets, and propose new regulatory sandboxes for individual products. This approach to regulation focuses on having no more or less regulation than is required to eliminate systemic risks and minimise consumer vulnerability, while still leaving breathing room for innovation. Some particularly necessary changes include modification of the legal requirements for stock exchange so that they cover digital assets, while maintaining compliance with anti money laundering and know-your-client requirements.

These legal modifications will bring financial law into the new era, and the regulators in Barbados are well underway to making these changes.

There are unfortunately a substantial number of drawbacks with cryptocurrency as well; As a person’s wallet is secured with a private key, there is a not insignificant number of hackers that will attempt to steal the key to make off with the data; as the keys are anonymous and not regulated by any governing body, they are also susceptible to theft with little recourse.

The anonymity also lends itself to shadier uses, with the well known and very large Silk Road website being an example of people being able to buy drugs, weapons, and other illicit substances and services with no legal oversight.

Another massive issue is one of energy use; as it currently stands the popularity of bitcoin has led to huge racks and data centres full of servers mining bitcoin, which uses huge amounts of energy. This has gotten to a point that not only is there little profit to the venture with the amount of money required to buy hardware and keep up with energy requirements, but it also has a very large carbon footprint.