

# IT Technologies

---

## Cloud Services/Servers

### What does it do?

Cloud Computing is an Emerging Technology that is revolutionising IT infrastructures and flexibility and has become a new paradigm for hosting and delivering services over the Internet. There are three main service models of cloud computing:

**Software as a Service (SaaS)**, also known as cloud application, services, represents the most commonly utilized option for businesses in the cloud market. A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side. It can be a beneficial for start-ups or small companies that need to launch ecommerce quickly and don't have time for server issues or software, vendors manage all potential technical issues, such as data, middleware, servers, and storage, resulting in streamlined maintenance and support for the business.

**Platform as a Service (PaaS)**, provide cloud components to certain software while being used mainly for applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain management of the applications. It is similar to SaaS, except instead of delivering the software over the internet, PaaS provides a platform for software creation, giving developers the freedom to concentrate on building the software without having to worry about operating systems, software updates, storage, or infrastructure.

**Infrastructure as a Service (IaaS)**, provides the same technologies and capabilities as a traditional data centre without having to physically maintain or manage all of it. You can purchase resources on-demand and as-needed instead of having to buy hardware outright. However, it is fully self-service for accessing and monitoring computers, networking, storage, and other services. Anytime you are unsure of a new application's demands, IaaS offers plenty of flexibility and scalability.

The main enabling technology for cloud computing is virtualization, which is the process of creating a software-based, or virtual, representation of something, such as virtual applications, servers, storage and networks. It is created using virtualization software to divide a physical (bare metal) server into multiple virtual servers.

Cloud servers are built, hosted, and delivered via a cloud computing platform via the web, and can be accessed remotely through any device with an internet connection.

Some examples of new state-of-art technology being developed using a cloud technology include:

**Microsoft Azure** is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centres.

**Google Cloud Platform** is service is suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search, Gmail, file storage, and YouTube.

**Salesforce** is the leader in cloud computing, offering applications for all aspects of your business, including CRM, sales, ERP, customer service, marketing automation, business analytics, mobile application building, and much more.

**IBM Cloud** provides a full-stack, public cloud platform with a variety of products in the catalogue, including options for compute, storage, networking, end-to-end developer solutions for app development, testing and deployment, security management services, traditional and open-source databases, and cloud-native services.

Cloud hosting is the single most effective way to reduce IT expenses while boosting efficiency. However, cloud technology is currently at its infancy.

The latest trends in cloud computing include Artificial Intelligence (AI), Hybrid Cloud Computing, Quantum Computing, Serverless Computing, its popularity is increasing at a rapid rate and it is predicted that this technology will virtually replace traditional data centres within the next three years.

The 5 innovative trends in Cloud Computing that can benefit small to large businesses altogether:

- The Emergence of Digital Natives in the Workforce.
- Artificial Intelligence (AI)
- Hybrid Cloud Computing.
- Quantum Computing.
- Serverless Computing.

### What is the likely impact?

Cloud computing reduces the expenses of the company as the resources are only acquired when needed and only paid for when used as the billing model works as per usage and there is no up-front cost. One of the concerning ongoing issues is any time you store data on the Internet, you are at risk for a cyberattack.

This is particularly problematic on the cloud, where volumes of data are stored by all types of users on the same cloud system. This issue can be overcome through getting up a Virtual Private Network, allows you to create a secure connection to another network over the Internet.

On a larger scale, AI capabilities are working in the business cloud computing environment to make organizations more efficient, strategic, and insight-driven. Artificial Intelligence is the future of technology and Cloud computing is already gained popularity and can continue the same. Integration of Artificial Intelligence and Cloud computing can create wonders and can become new technology.

### How will this affect you?

It has not only impacted our lives but also how businesses and organizations manage their data and customers. Cloud computing offers access to data storage, processing, and analytics on a more scalable, flexible, cost-effective, and even secure basis than can be achieved with an on-premises deployment.

Cloud computing can offer a competitive edge over competitors. It helps you to access the latest and applications any time without spending your time and money on installations.

Rather than purchasing expensive systems and equipment it can reduce my cost as a business by using the resources on the cloud. Hosted virtual desktops are used to access files from anywhere, at any time, cloud computing enables employees to work remotely.

# Cybersecurity

## What does this technology do?

Cyber security is the protection of computer systems from theft and damage to the hardware, software, disruption or misdirection services, data, damage, or unauthorised access.

## What does it do and why is it important?

Cyber-attacks not only effect large scale organisations and government bodies but also small size businesses and common people like us. In today's era, I. D thefts, credit card fraud, email internet fraud, theft of corporate data, cyber extortion, ransomware attacks etc have become so common that a report by at the University of Maryland suggests that "hackers attack a computer in the U.S every 39 seconds on an average". As our reliance on A. I, cloud computing grows the need to protect our valuable data is more than ever. It would not only protect law-abiding citizens, small businesses as well as multinational private and public organisations from cyber-attacks that could steal personal as well as valuable customer's information, but it would also protect top secret military and government information from being misused by hackers and terrorist organisations.

## Cyber security at present:

Security related to the I.T sector has become a major concern for our banking, financial services, defence, and aerospace as well as other important sectors. Recent development in the A.I, machine learning sector has without a doubt revolutionised the way organisations do business and manage enormous amount of data but at the same time has exposed them to cyber-attacks.

According to a recent report by European cyber security organisation, the government of U.K invested around \$2.30 B USD for the implementation of cyber security programs in defence and research sector. Furthermore, in response to the rise in intense threats and breaches governments across the world are emphasising on increasing investment in defence and research sectors to establish advanced and well protected cyber security infrastructure.

Companies in the cyber security market are adopting technologies such as IoT, machine learning and huge amount of data in their security business units. Most of the companies in the market are shifting from a "signature based" malware detection system to an IoT enabled machine learning signature less system. Big data technology on the other hands is playing an important role by assisting big organisations understand and analyse potential risks.

Cloud computing has also played a significant role in the growth of cyber security industry. Cyber security solutions are based on complex mathematical models and often deals with handling huge amount of data. Cloud computing has offered a safe, reliable, low-cost platform to monitor this data. This has helped organisations to detect any uncertain threats quickly.

## What is the likely impact?

With emergence of disruptive technologies such as Artificial Intelligence, IoT, block chain and others. Cyber security sector has evolved drastically in the past 20 years. The next 5 years look quite promising for the industry and it's predicted that the sector will keep growing as the demand to hire specialised cyber security personals to counter the increase in cyber-attacks. According to statistics global cyber security market is predicted to grow from \$167.1 B USD in 2019 to \$248.67 B USD by 2023.

Additionally, the adoption of cyber security technology is only expected to grow further with an increase in investments from nations like India, Spain, Canada, South Korea etc. At the same time the requirement from our healthcare, defence, aerospace, financial services and manufacturing sector has only contributed to the growth of cyber security in the recent years and it is estimated to only increase in the next 5 to 10 years.

## Impact of Cyber security on our future

The recent developments have without a doubt revolutionised the way we interact with technology around us. On one hand A. I and machine learning has made everything so convenient that with just a voice command

we can control and operate electronic equipment at our homes and in our hands. With the help of voice to text technology we can send messages, emails etc. With the help of biometrics technology such as face recognition we can make payments and authorise devices to perform important tasks on our behalf. Today A.I and machine learning algorithms can be used to automate tasks that make decisions much faster and quicker hence as a result increased productivity with a very low margin of error. In the financial services or the banking sector use of A.I to resolve most of the issues raised by customer is already proving to be effective.

On the other hand, we cannot ignore the fact that the A.I technology also create cyber security risks and machine learning algorithms can be easily manipulated by hackers .In short nobody can tell what the next major cyber-attack will be or where it will come from, and as small to medium businesses as well as common people like us are becoming aware of these threats the demand of having a strong, reliable cyber security infrastructure has only been predicted to grow higher in the near future.

The other major future impact of cyber security on our society that we may have is a growing risk of cyber war fare. The trend began in 2010 with Stuxnet. By 2017 a Russian backed hacking group was boldly going after big American corporations. As more nations become nuclear states these types of attacks are more likely to increase and combat ware to reduce. This would require stronger and much more efficient cyber security defence system, and this may trigger a race among the nations to make it a part of their defence budget and start investing int it heavily.

### How will this affect you?

With going frequency of cyber-attacks year after year the need of protecting ourselves from these attacks is more than ever. I believe students at a very early age should be educated on the risks associated with cybercrimes and should be taught basic cyber security skills.

Current projection suggests that the global market will be worth over \$42 billion by 2022 however there is only so much a paid for software can do to protect businesses.

Larger security spends do not achieve anything unless they are monitored by someone with adequate information security skills.

The shortage of workers with these skills has created a huge gap in the market. A study by the global information security workplace estimated a gap of 2 million jobs by 2022.

Personally, as an individual who is passionate about cyber security and someone who's interested in working in the industry this gives me the confidence that after graduation and after attaining the required certification the possibility of getting into the industry is quite high in the future.

As the number of attacks will keep increasing so will be the requirement of people with the skills to counter those attacks. Even if A.I is introduced in the information security there will always be a need for the professionals to protect that A.I from getting manipulated.

## Autonomous Vehicles

### What does this technology do?

Autonomous vehicles are cars or trucks that are able to operate without input from a human driver, and never require a human to take control and intervene to safely operate the vehicle. Autonomous vehicles rely on sensors, actuators, complex algorithms, machine learning systems and powerfully processors to execute software. (Synopsys.com, 2021).

Autonomous vehicles are able to use sensors located in different parts of the vehicle to create a map of their surroundings and use video cameras to check for pedestrians, vehicles and other obstacles. These cameras can also detect stop signs and read the instructions presented by traffic lights. Vehicle detection is enhanced by the use of radar sensors. Lidar sensors send pulses of light to detect road edges identify lane markings and measure distances.

These sensor inputs are then processed by sophisticated software which plots the required path and manipulates the acceleration, braking and steering to achieve the objective. Hard coded rules, obstacle avoidance algorithms and predictive modelling help ensure that the software operates the vehicle safely and remains in compliance with traffic rules and regulations.

Advanced autonomous vehicles are connected and capable of communicating with other vehicles or infrastructure such as new model traffic lights programmed to send instructions directly to autonomous vehicles without relying on a video camera to interpret the light signals.

There are currently no fully autonomous vehicles available, however testing is taking place. Partially autonomous vehicles are available and are classified by the following system based on their degree of autonomy (Hecht, 2018).

- Level 0: All major systems are controlled by a human driver
- Level 1: Most systems are controlled by a human driver but some ancillary systems such as cruise control or automatic braking may be controlled by the car. Only one automated system can function at any given time.
- Level 2: The vehicle is capable of two or more simultaneous automated functions, such as steering or acceleration but a human driver is necessary for safe operation.
- Level 3: The vehicle is capable of managing all safety critical functions under some conditions but a human driver must be present and take over when alerted.
- Level 4: The autonomous vehicle is fully autonomous in some driving scenarios but not all
- Level 5: the autonomous vehicle is capable of self driving in every situation.

Oxbotica in the United Kingdom is currently performing a government backed effort to test a fleet of six Ford Mondeos. The cars will operate on a nine-mile circuit from Oxford parkway station to the main train station in the in both day and night conditions.

Progress continues towards level 5 fully automated autonomous vehicles however progress from level 3 to level 4 and 5 has been slower than expected and slower than the rate of progress from level 0 to level 3. Earlier estimates of level 5 fully automated autonomous vehicles being available and common in 2020 have proven overly optimistic and current estimates for achieving level 5 autonomy suggest decades rather than years.

### What is the likely impact?

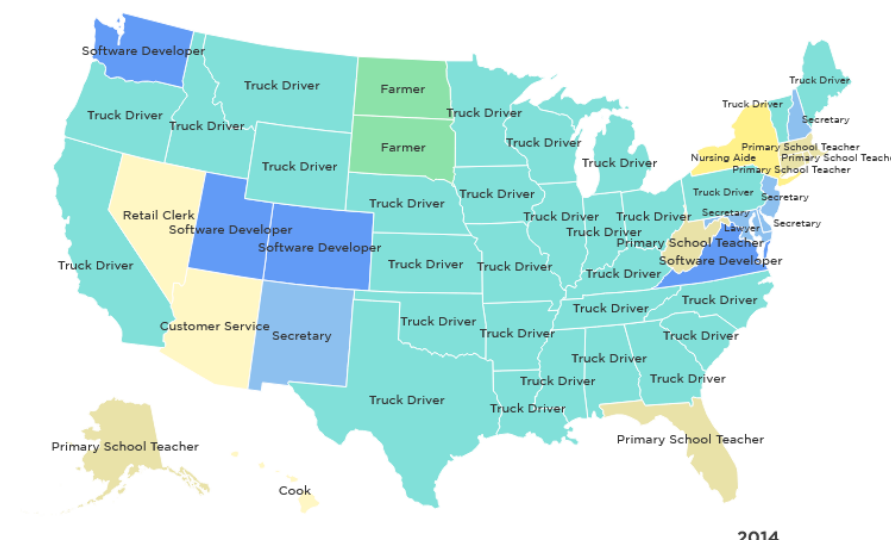
The impact of widespread adoption of autonomous vehicles could potentially be significant for our society. It is believed that self-driving cars will significantly reduce crashes and thereby decrease injuries and fatalities. Autonomous vehicles can move faster and more safely than conventional vehicles and could drive closely to each other to reduce air resistance. This coupled with decreased accident-related disruptions may reduce congestion and allow for more efficient transportation. Increased efficiency in our transportation network would decrease our energy consumption and pollution output which would be a significant environmental benefit.

To help illustrate the potential positive impact of autonomous vehicles PWC (2013) estimates that in the United States of America autonomous vehicles may reduce vehicle accidents from 10.8 million per year to 1.1 million. They further estimate the widespread adoption of autonomous vehicles will reduce the American fleet from 245 million down to 2.4 million and also reduce the transport related yearly energy consumption from 19 billion gallons down to 190m gallons. (PWC, 2013) It is also worth noting that autonomous vehicles can make transportation more accessible by giving people who are unable to drive the ability to use our motorways.

As with any change of this scale, there will likely be significant negative impacts as a new disruptive technology is adopted. The potential for job losses is notable. The Bureau of Labour Statistics lists that almost a million people in the United States of America are employed in motor vehicles and parts manufacturing with an additional three million people employed in the dealer and maintenance network. Truck, bus, delivery and taxi drivers account for nearly 6 million professional driving jobs. Virtually all of these ten million jobs could be eliminated in the next ten to fifteen years, and this list is by no means exhaustive. (Kantor, Z, 2015)

It is worth noting that these industries are dominant in many parts of the United States of America and communities affected by these disruptive changes may be less able to move to any employment opportunities required by the emergent autonomous vehicle industry.

**The Most Common\* Job In Each State 1978-2014**



(Quoctrung Bui, 2015)

### How will this affect you?

I believe that the primary effect autonomous vehicles will have on me is to reduce the cost of my transportation. Traditional car ownership is very inefficient due to the small amount of time you actually spend driving your car. The RAC foundation in the United Kingdom estimates that the average car is parked at home for 80% of the time, parked elsewhere for 16% of the time and is only on the move for 4% of the time. (RAC, 2012). If we move to a transportation model where car ownership is rare and people instead hire self-driving cars on an on demand basis the cost for our transportation could decrease.

Autonomous vehicles would also increase my opportunity to be productive as time spent commuting to work or between appointments could be used for study or meetings rather than paying attention to the road. Americans spend an average of 293 hours driving per year, which is equivalent to over seven 40 hour work weeks. (Adorney, 2019). If even a portion of this commuting time can be converted to productive activity then the personal and economic benefits would be significant.

I would also appreciate the improved peace of mind when commuting due to the improved safety outcomes full implementation of autonomous vehicles could bring. In the United States of America the National Highway Transportation Safety Administration found that somewhere between 94% and 96% of all motor vehicle accidents are caused by some kind of human error. (NHTSA, 2016). Even if you consider yourself an above average motorist you always have to be careful of what other

drivers are doing and could be involved in an accident through no fault of your own. Replacing the average driver with an autonomous vehicle would make everyone much safer.

## Blockchain and Cryptocurrency

### What does it do?

A Blockchain is a distributed ledger that is immutable and does not give trust to intermediaries. Instead of trust, Blockchains use mathematics, namely cryptography to secure the transactions and to validate them amongst users. Information stored inside blockchains cannot be removed once it has been written. Changes to the blockchain can only occur if a consensus is met amongst the participants in the network.

A distributed ledger means that the full ledger is distributed amongst all the nodes in a network. A node being a computer in which the ledger is copied onto. Blockchains can be audited with relative ease as the ledger can be accessed through any of the nodes. There is no one person in charge of a blockchain.

Blockchains are immutable and therefore cannot be changed in anyway once it has been verified. The block contains some identifying information such as a timestamp, a hash and the hash of its parent. The hashes that are given to blocks are unique and if a block is altered, it is easy to find as the children to the altered block become invalid. The child block contains the hash of its previous block (parent block) and each subsequent block contains the hash of its parent and so on. It is very difficult for a blockchain to be tampered with or falsified. Because any changes to a blockchain needs to be verified and validated via a consensus among nodes in the network, it is extremely difficult to hack.

Blockchains allow for quicker, trustworthy and reliable transactions to occur. This is due to a blockchain being decentralised. By removing intermediaries, transactions can occur peer to peer (P2P) which are a lot faster than a conventional centralised system. The security that blockchains provide, using cryptography, computer-generated addresses and the need for consensus, allows users to buy and sell P2P without the fear of transactions being exposed.

Blockchains achieve this by using what is called Distributed Ledger Technology (DLT). Rauchs et al. (2018) defines a DLT system as 'a multi-party system in which participants reach agreement over a set of shared data and its validity, in the absence of a central coordinator' and that the differences between DLTs and more traditional distributed databases are 'rooted in designs capable of supporting data and maintaining data integrity in an adversarial environment.'

Crypto currency is a form of electronic money. Cryptocurrencies such as bitcoin are still in the early stages in terms of usage. Cryptocurrencies have broken away from their initial stigma of being used for black market transactions, and instead have started to be acknowledged for their capabilities in allowing P2P transactions without the need of an intermediary.

An example of a blockchain and cryptocurrency is Bitcoin. Bitcoin is a cryptocurrency that utilises blockchain to maintain and record its transactions. Users can send each other bitcoin and all transaction information are stored inside a blockchain. Users are also incentivised by bitcoin rewards for verifying blocks in the blockchain. This incentive helps to keep Bitcoin regulated and legitimate.



### What is the likely impact?

Blockchain is still in early stages of understanding what it could be used for and what sectors could make use of blockchains to their advantage. Zheng et al. (2018) discusses the future possibilities of blockchain in regard to areas such as Smart contracts and Artificial intelligence (AI). Smart contracts function as 'digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution' (Cong and He 2019, p. 9). Zheng et al. (2018) notes that analysis on smart contract attacks such as the attacks on the DAO which resulted in \$60million dollars' worth of cryptocurrency being stolen is very important as well as the performance of smart contracts. As the use of blockchains becomes more prominent, the use of smart contracts will also rise and as such, smart contracts must also be reviewed for security and viability within the blockchain.

Zheng et al. (2018) also discusses the future use of AI in determining if contract conditions have been met. They note further that AI could be used instead of a third-party to 'build an intelligent oracle'. An unmanned AI that is not controlled, self-teaches and self-trains in order to solves challenges in regard to contracts made using blockchains.

There are many real-world implications due to blockchain. The immutability, transparency and efficiency of blockchain is what makes it a system which can be adapted and have an impact on other fields and markets. An impact of blockchains is the removal of an age-old currency known as trust. Trust is something that has been given to organisations and institutions which have acted as a centralised intermediary. Blockchain relies on cryptography and the incentives it provides users to create a system that can be trusted based on the shared responsibility amongst its users.

Applications made using blockchains have allowed for safer, transparent, authentic and more secure transactions. A paper researching the impact of blockchain technology on business models in the payments industry found that blockchain will likely have an impact on three services within payments. Enabling direct transactions peer-to-peer, improvement of international transactions, which will 'erode [currency exchange] as a service' and the use of smart contracts linked to business transactions. (Holotiuk, Pisani & Moormann 2017). Casey et al. (2018, pp. 18-19) also gives mention to the improvement of cross-border payments as an impact of blockchain and DLTs.

Blockchains applications spread further than just cryptocurrencies and P2P transactions. Blockchains and their capabilities and security have attracted other markets in which they are being applied. A few examples of other ways blockchain has been applied is by a company called SimplyVital Health who aims to use blockchain as a means for better health data management. It is also being used in the diamond trading industry with the development of Tracr, a blockchain platform that records and tracks a diamonds life cycle from mine to jeweller, providing transparency, peace of mind and authenticity. Ubiquity is a real estate recordkeeping platform that utilises blockchain for the record of ownership. Pharmaceutical companies are even making use of blockchain to provide indelible records of transactions as well as data which demonstrates the following of regulations in the MediLedger project.

### How it will affect you?

As blockchain and the use of cryptocurrencies is still in the early stages of making its way into the mainstream, it is difficult to say how it will affect us in this day and age, some of the services mentioned above are pilot projects and have the possibility to become the standard for storing and sharing information or data.



Blockchain and its capabilities have established foundations in P2P networks for 'sharing, exchanging and trading digitized information, goods and assets.' (Caradonna, 2020 p.47). These foundations are the building blocks that can show the general public how to transact and share without the use of an intermediary.

If the public is taught how blockchain can be used in a way that benefits them, they will feel more inclined to use it. As example as mentioned above being for management of medical records and health data. People's medical records are stored at the institution or hospital you attend, and this cause your medical data to be scattered. Using blockchains to maintain your health data can allow for your data to easily accessed as well as the data being held securely. In the circumstances where you are unable to provide medical professionals with your allergies and other information, a health data blockchain can provide professionals with your data regardless of the institution you go to.

In its essence, blockchain is not a technology which directly effects the end user. It is a technology which works in the background assisting us. A case in where blockchain is being used to effect the end user is food distribution. (Bumblauskas 2020) explores a use case of blockchain as a way to trace eggs from the farm to the consumer. A consumer only scans a QR code on the packaging and it provides access to data from its journey to the store.