GLOBAL IDENTIFICATION IN THE CLOUD: A STUDY OF CLOUD PASSPORT MODEL

By

Yuk-Tung Tonnie Lam

A Thesis Submitted to Macquarie University

For the Degree of

Master of Research

Department of Computing

Faculty of Science and Engineering

October 2017

MACQUARIE University

SYDNEY·AUSTRALIA

Declaration

I certify that the work in this thesis entitled "Global Identification in the Cloud: A Study of Cloud Passport Model" has not previously been submitted for a degree nor has been submitted as part of the requirements for a degree to any other university or institution other that Macquarie University. I also certify that the thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been appropriately acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Yuk-Tung Tonnie Lam

Acknowledgements

Firstly, I would like to thank my family, for I would never have been able to finish my dissertation without their support.

I thank Ms Claudia Butera who helped proof-read the drafts of the thesis.

My special thanks to my supervisor, Dr Peter Busch, for his guidance and encouragement during the preparation of this thesis.

Finally, I would like to dedicate my work to Jesus the Mighty God and my Savior, as “all wisdom comes from the Lord, and so do common sense and understanding” (Proverbs 2:6-8 CEV).

Abstract

In this research, we studied the idea of Cloud Passport, an initiative which uses the latest technologies to replace physical passports. Advantages and challenges of implementing a passport-less system for travel between countries were discussed. Different types of technology adoption models and research method were evaluated. A Cloud Passport adoption model was formulated as the basis for the current research.

A convenient sample survey was conducted in February 2017 to Australian adult Facebook users to find out the social attitude on the proposal of Cloud Passport. Survey results showed that there was a 70% acceptance level on Cloud Passport. Social opinions on different technical components of Cloud Passport were also asked in the study. 75% of the interviewees thought that Cloud Passport would be available worldwide in the next 10 to 20 years. A textual analysis of the feedback from the survey discovered some drivers and barriers to the implementation of Cloud Passport.

The observations from the surveys formed an overall view of the social opinion of a sample of Australians on the Cloud Passport initiative, which may help to contribute further study for an appropriate change management strategy for a successful roll-out of Cloud Passport in Australia.

Keywords: Cloud Passport, IDaaS, BaaS, Biometrics, Cloud Computing, Identity Management, Security, Border Control

Contents

List of Figures

List of Tables

This Page Intentionally Left Blank

Chapter 1 – Introduction

1.1 The global situation regarding international travel

Since the inauguration of the first commercial airline flight in 1914 in the US (Sharp 2012), aeroplanes have been a favourite type of public transport to bring people from one country to another. With the advances in aviation technology, one would expect that more and more people will take aeroplanes to travel overseas than another type of transport.

By looking at the yearly airport traffic statistical figures from Airports Council International (ACI), the volume of traffic at border control for all countries has increased by around 4% to 6% between 2014 and 2016 (Wikipedia 2017). A summary table of the Year-on-Year (YoY) increase of passengers handled by the top 50 airports is shown in Appendix B.

With the increasing number of passengers travelling by aeroplane, the processing of baggage check-in, as well as the efforts required to board passengers and baggage to their corresponding aeroplanes have increased significantly. With an estimated 3.7% annual Compound Average Growth Rate (CAGR) in global traffic, and a projected 7.2 billion passengers in 2035 (IATA 2016), the strain to the demands to handle travellers in airports in the world will only get worse as time goes on.

U.S. Customs and Border Protection has ordered a survey titled "Primary Inspection Wait Time at U.S. Ports of Entry" (Roberts et al. 2014). Survey results showed that the average wait time for passengers in ports of entry has increased by around 25% from 2010 to 2013, with the average wait for non-US residents at almost twice as high as for US residents (Roberts et al. 2014). With the forecast travellers growth rate of 4.7% for non-US resident arriving in the US between 2013 to 2018 (Roberts et al. 2014), even worse waiting time to US ports is predicted for the near future. The increase in the waiting time at border control will also happen in the other main cities like Sydney airport

Besides the need for passengers to transfer between flights, the logistics to accommodate aircraft movements, as well as the efforts to manage retail shops and food malls in an airport where the need to be reviewed to cope with the ever-increasing demands from the increase of passengers (Kalakou et al. 2015). The primary stakeholders like airport owners, operators, airlines, commercial shop owners, as well as security and border control agencies need to work together closely (Kalakou et al. 2015), to ensure benefits for all parties as well as the passengers in the airport.

1.2 Australian situation

Sydney airport, as the busiest airport in Australia (Airport Traffic Data 2017), has a year-on-year growth in passenger numbers passing through the airport border. A table of the top 10 Australian airports is shown in Appendix B.

In the newsletter released on 20th January 2017, Sydney Airport Managing Director and CEO Kerrie Mather said, "2016 was an outstanding year, with international passenger growth of 8.9%. 2016 was the

fastest growth rate we've experienced in 12 years and the strongest total passenger traffic growth for six years" (Sydney Airport 2017, 1st paragraph).

With the recent announcement to build a new airport at Badgerys Creek, airports in Sydney will be able to handle an extra 10 million passengers per year in 2026, with a projected capacity of handling 82 million passengers when the new Sydney airport is in full operation in 2064 (O'Sullivan 2017).

Among the list of stakeholders for airport operations, security and border control agencies play a significant role in the handling of passenger processing in airport terminals.

According to the Australian government website, the role of Australian Border Force officers is "to protect our border and manage the movement of people and goods across it and, by doing so, we aim to make Australia safer and more prosperous" (Australian Border Force 2017, 1st paragraph).

The scope of work by Australian Border Force are (but not limited to) the following tasks (Australian Border Force 2017): to review passports and other travel documents as travellers arrive and depart Australia; to question arriving and departing passengers, and conduct search baggage for prohibited or restricted goods; to search aircraft or vessels for prohibited or restricted goods such as weapons, wildlife, products made from endangered species and counterfeit goods, and seize the items when needed.

Australian Border Force is joining forces with intelligence, law enforcement and other agencies, to increase throughput for protecting the border of our countries (Australian Border Force 2017). As the number of people travelling in and out of Australia ports increase, there is a need for more resources in the border control function of the country. Like all other border force agencies in the world, the Australian Border Force is continually facing a dilemma: to cope with an increasing demand of passengers to pass through Australian borders without significant delays, while preventing potential terrorists and violent extremists from entering Australia.

1.3 Identification standards globally, timeline approach

The need for a passport for travel started after the Great War in the 1920s (Clark 2011). During that time nations realised the need for "documentary substantiation of identity used to register and keep watch over aliens". A paper-based passport then started progressively worldwide for travellers. From 1960 onwards, as more people travelled by air, and with the advancement of computer technology, automation of passport processing was sought for a more efficient border control service. A new type of passport - a machine-readable travel document (MRTD) was introduced in Australia in 1983 to cater for the need at that time (Clark 2011).

With increasing mobility of people around the world and the rising threat of terrorist activity in different countries, there is a strong need to have a more robust way to identify travellers (Kalakou, Psaraki-Kalouptsidi and Moura 2015). The 9/11 incident in the US in 2001 prompted the urgent need to have tighter border control against potential terrorists amongst travellers (Jones 2011). In 2005, a new form of passport with biometric information called e-Passport began to roll out in Australia (Australian Passports Determination 2005). Nowadays e-Passports (or Passport cards in other countries) are widely

used throughout the world. The *International Civil Aviation Organisation* (ICAO), a UN agency that formulates the principles and techniques of international air navigation, planned that by 2020 all nations should be ready to implement an ICAO-compliant e-Passport (ICAO Traveller Identification Programme – TRIP 2015). The evolution of travel documents in Australia is shown in figure 1.1.

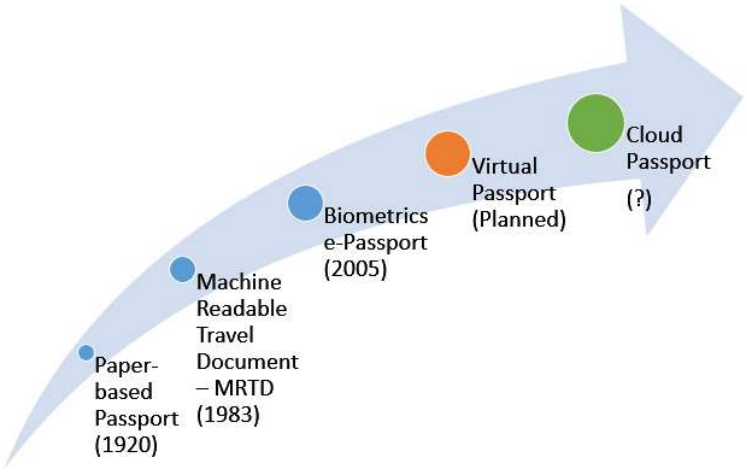


Figure 1.1 - The Evolution of Travel documents in Australia (source: Clark 2011)

With the announcement of the concept of "Cloud Passport", the Australian *Department of Foreign Affairs and Trade* plans to introduce a paperless Virtual Passport between Australia and New Zealand as a start (Lynch 2016). Whether this initiative will eventually be embraced by other countries with automatic border control (ABC) installed is still yet to be seen. Michael Lynch, director of *Department of Foreign Affairs and Trade*, explained in a paper the vision of a Virtual Passport for the Trans-Tasman arrangement (Lynch & Bennett 2015). A picture to represent the evolution of travel document in Australia is shown below.

1.4 Technological development of global passports

The manual-based process to check passengers' passports and security profiles at border gates are not sufficient for a large volume of travellers and could be the cause of delays in processing time within a limited human resources level. In order to increase the throughput of the processing at border gate, as well as limiting costs at the same time, an innovative and effective vetting process is needed for border control at airports and seaports. The advancements in technology help border control agencies to invent new ways to identify and authenticate a passenger, with minimum human resource needed, while trying to keep a seamless travelling experience.

SmartGate, an electronic border control system was introduced to Australia in 2007 (Sharma 2007), performs self-service passport control checks electronically. Travellers with an approved e-passport, from a list of designated countries (Arrivals SmartGate 2017), can use SmartGate for faster passport checking at border control. On the other hand, SmartGate helps border control authorities reduce the queuing time for passport processing, as well as to provide a better security control at the border gates (Ewing 2015).

In 2017 Australian Customs and Border Protection will start to replace the existing Border Gates in airports and seaports, with a new 'Vision Box Machine' which captures the facial biometrics information of passengers when they pass through the corridor of the border control (Nash 2017). Facial recognition is then performed between the captured biometric data, and the biometrics information in the e-passports through contactless technology. The aim is to have 90% of travellers use the latest version of automated border control system by 2020 (Nash 2017).

Apart from the above initiatives for better border control, an idea to eliminate the need of carrying a passport by using the latest Cloud technology emerges.

1.5 Criteria for the Introduction of Cloud Passport in Australia

In a news report of October 2015 (Quinn 2015) announcing the winners of Australian Government's Innovation Exchange project, Julie Bishop, Australia's Foreign Minister, introduced a new initiative of "Cloud Passport", which enables travellers to travel to countries without the need of a physical travel document. Minister Bishop said the concept of storing the data of passengers for biometric identification online and being available in the cloud could 'go global' (Quinn 2015). It was a grand vision of travelling freely without identification documents all over the world, without compromising the tight security control when travellers pass a country's border.

To build a Cloud-based digital passport system for automatic border control, one needs a set of the following new technologies: a more advanced automated border control system to handle cloud-based data; a globally accredited biometrics-based identification and authentication model; and a Cloud-enabled secured data exchange infrastructure to allow secure data transmission between countries.

However, the criteria of whether physical passports can be eliminated are mainly determined by advancements in technologies (such as cloud, security and encryption, globally secured communication link). On the political perspective, it is also determined by the readiness of embracement of new technology by the public, and cyber-security readiness for border control by governments in various countries.

1.6 Research Objectives

The aim of this thesis is to find out the level of acceptance on the proposal of Cloud Passport by the sample of the Australian public. The collected opinions can help to build an appropriate change management strategy, and hopefully a successful roll-out of Cloud Passport in Australia.

The research question is stated as follows:

> *"Given the current level of technology that enables a Cloud Passport model - what are the opinions of select members of the Australian general public to the adoption of a cloud passport? What are the concerns of a sample of Australian with regard to replacing the current physical passport with a digital version?"*

The research objectives of the current thesis are to get answers to the research questions and to report on the findings on the attitudes of the general public on the vision of Cloud passport as an alternative for the current travel document arrangement.

The following paragraphs describe the layout of the thesis:

Literature Review

In chapter two, the components to implement a Cloud Passport system is then discussed in detail. The concept of biometrics identification as a Cloud service (BaaS) is then elaborated. This is followed by a proposal of the Cloud Passport model, with some analysis of the advantages and challenges if Cloud Passport is implemented. At the end of the chapter, the potential development of cloud passport in the future is examined.

Research Philosophy

In chapter three the building blocks to develop research philosophies was examined. Different types of research paradigms and their underlying philosophies are compared, with the corresponding research methods evaluated. Mixed method research methodology and a set of instruments based on the selected research methods is then proposed to develop a research framework for the research topic.

Research Methodology

In chapter four, the nature of the research topic and the details of instruments for data collection was listed, based on the research framework determined in chapter three. The design of the survey questionnaire and the rationale of the choice of the method of collecting sample data for the survey was then discussed. Methods for processing and analysing the data gathered, as well as the way to archive and remove survey data after the research is then considered.

Quantitative Result Analysis

In this chapter, the results of the survey questions were elaborated. The primary emphasis on the analysis of the survey results is to describe the results in a plain and unbiased way; to perform quantitative analysis on collected data for Question 1 to 16; to carry out bivariate analysis on collected data from a combination of two questions, e.g. Question 12 (acceptance of Cloud Passport) with data from Question 4 (different genders); and to state the observations from the survey results.

Qualitative Result Analysis

In chapter six, the results of the free text input field in Question 17 of the survey are analysed. The main emphasis on the analysis of the survey results are to describe the result in a plain and unbiased way; to perform a textual analysis of the free-form text question on the overall acceptance of implementation of Cloud Passport (Question 17) and to state the observations from the survey results.

Discussion of Survey Results

In this chapter, the summary of the analysis of the survey is discussed. Some findings and observations from the survey are then discussed in more detail, followed by listing a formal interpretation of the survey in response to the research question. At the end of the chapter, some suggestions for improvement of the survey method via social media is then discussed.

Conclusions

The last chapter of the thesis concludes with results of the research and states what the main accomplishments are against the original objectives in the research question. A review of possible areas for future research is listed at the end of the chapter.

References and appendices of the research are attached at the end of the thesis.

Chapter 2 – Literature Review

2.1 Introduction

Since the introduction of a physical passport in 1920 (Clark 2011), Australia has evolved to a version of e-Passport in 2005, of which biometric information (face and fingerprint biometric identification) are stored in a chip in the passport (Australian Passports Determination 2005). By adding biometric information in a passport, the risk of having an illegal entry of traveller using forged passports can be minimised (Australian Passports Determination 2005), and keep extremists (terrorists and people who are of potential national threats) from entering Australia. With the advancement of cloud technology and secure internet communication, an improvement in the way to deliver passport information is continually sought for even more reliable and efficient border control for Australia and globally.

A news report in October 2015 (Quinn 2015) announcing the winners of Australian Government's Innovation Exchange project - Julie Bishop, Australia's Foreign Minister, introduced a new initiative of "Cloud Passport", which enables travellers to travel to certain countries without the need of a physical travel document. According to the report in the *Daily Mail UK*, Minister Bishop said the concept of storing biometric identification data of holders online and being available in the cloud could 'go global' (Quinn 2015). It was a grand vision of travelling freely without identification documents all over the world, without compromising the tight security control when travellers pass a country's border. However, the criteria of whether physical passports can be eliminated are mainly determined by advancements in technologies (such as cloud, security and encryption, globally secured communication link). With regard to the political perspective, it is also determined by the readiness to embrace new technology and cyber-security readiness for border control by governments in various countries.

2.2 Australian Government approach to Virtual Passport

Lynch described the Australian approach for a Virtual Passport in detail (Lynch & Bennett 2015, Lynch 2016). Both Australia and New Zealand have the political will to implement a frictionless border-crossing arrangement for a tighter relationship. The primary criteria are (Lynch & Bennett 2015):

- Currently, the scope is for travellers between Australian and New Zealand only
- Both countries have already implemented an Automated Border Control system (SmartGate for Australia and New Zealand)
- Both countries have already issued ICAO compliant e-Passports
- Australia and New Zealand have a trade agreement to make travelling between the two nations as streamlined as possible – i.e. a more "domestic like" travel arrangement

How does a Virtual Passport system work?

- A virtual ID (virtual passport) is used instead of a paper-based passport, which can uniquely identify a person from biometric information

- The traveller's face - a type of biometric information, becomes the virtual passport identifier
- Biometric template data is stored securely in a back-office system in the Australian and New Zealand government's offices
- Travellers need to opt-in for the virtual passport (with passenger's biometrics info as well as visa information) to be transferred to the destination country as a pre-flight arrangement
- The virtual passport information of the traveller is transferred as a data packet from the source to the destination country through a data package in advance
- A one-time key is generated to the traveller to access the virtual passport information
- The traveller presents the one-time key of the virtual passport for visa application, ticket booking and the check-in process
- At immigration of the departing country, the face of the traveller is checked against the pre-loaded biometric data of the traveller at the SmartGate. Once the identification is validated, the traveller is then allowed to pass the gate and move on
- At the destination country, the face of the traveller is identified by comparing the captured biometrics information of the traveller against the database in destination's border control system, of which with the biometrics information of the traveller pre-populated before. Once the traveller is identified and validated with the checklist in the destination country, the automated border control system will allow the traveller to pass through and enter the country.

2.3 Advantages and Challenges of Virtual Passport

According to Lynch and Bennett (2015), the introduction of a virtual passport can improve security as well facilitate border management of a country. Below are the advantages of the virtual passport in comparison to the current physical passport (Lynch & Bennett 2015):

- Virtual Passports are hard to forge
    - Compared to the physical passport, a virtual passport is hard to be forged and altered.
    - It also cannot be lost or left in the wrong hands, as passport information is securely stored in a back-office system of the Border Protection authority of the issuing country
- Allow pre-screening of a traveller's profile
    - A comprehensive set of travellers' high-quality biometric data can be obtained by the destination country in advance through the virtual passport system, thus enabling the destination country to carry out more advanced pre-screening of travellers' information against watch lists
- Better face recognition techniques
    - Technology advancement, as well as the improved algorithm for identifying a person, enable automated border control gates (SmartGate) to perform better in False Recognition Rates (FRR) and False Acceptance Rates (FAR) when compared with manual identification by a border control officer (White et al. 2014)
- Faster processing time, better service

    - The processing time for a low-risk traveller is shortened. Thus it improves the average processing time for travellers passing through border control and should lead to better traveller satisfaction levels
- Cost savings:
    - Potential savings in time and human resources, hence leading to financial savings for border processing

In conclusion, the implementation of a virtual passport can improve the efficiency of border control operations, as well as an improved security check for border protection of the destination country.

On the other hand, the concept of a virtual passport did not address some of the common issues that can happen to a traveller (Kalakou et al. 2015). Some of the potential challenges for virtual passports are listed below (Kalakou et al. 2015):

- A manual opt-in approach may lower acceptance rates:
    - The opt-in approach of providing the itinerary by a traveller to border control is primarily based on the traveller's efforts to enter their itinerary manually.
- Ticket bookings do not require a passport:
    - The virtual passport, together with visas, could be packaged to form a "digital travel portfolio".
    - The traveller can then use the digital travel portfolio to book tickets and perform a check-in for a flight.
    - The real-life situation is that there is no need to have a valid visa when you make a booking for an airline ticket.
    - The airline only verifies your visa and travel document at the time you are checking-in for the flight.
    - So the need for accessing a Virtual Passport when making a ticket booking is not required
- Inflexibility in coping with a changing itinerary:
    - As the digital travel portfolio of a traveller is sent to destination countries in advance according to the itinerary entered, it will become inflexible if a traveller needs to change his/her itinerary due to ad-hoc or unexpected circumstances.
    - For example, the change of flight destination by the airline due to weather or some security threat to another airport.
    - So the traveller probably needs to carry a physical passport, just in case

To eliminate shortcomings of the virtual passport, an online and on-demand approach in delivering the digital travel portfolio is needed, to (or "intending to") cater for changes in the itinerary as well as improve the user's experience when interacting with the new virtual passport system.

With the advancement of current cloud technology as well as a robust and secure global Internet link, one can improve the virtual passport to make use of the latest cloud technology, and form a genuinely subscription-based identity and access control service – i.e. the introduction of an authentic Cloud

Passport system. Before proceeding with the details of a Cloud Passport, one needs to address the concept of cloud computing, Identity and Access Management (IAM), Biometrics identification and Biometrics-as-a-service (BaaS) in the next section.

2.4 Cloud Computing and Cloud Services

Cloud computing has become a mainstream model in business due to its scalability of cloud system resources, and an on-demand subscription-based billing model (Busch et al. 2014). So what is cloud computing? A possible definition provided by Baun et al. (2014) is as follows:

> By using virtualized computing and storage resources and modern Web technologies, cloud computing offers scalable, network-centric, abstracted IT infrastructures, platforms, and applications as on-demand services. These services are billed on a usage basis (page 3).

The ideas of cloud computing are resource sharing, computer virtualisation, elastic or scalable service capacity, on-demand and instant service which is always available, and billing by units of usage (pay-as-you-go) (Khorshed, Ali and Wasimi 2012). According to the Australian Government Cloud Computing Policy (2014 edition), the essential characteristics of cloud computing are as follows:

- On-demand self-service: a client can control how much server time and network storage capability they require without the help of service providers
- Broad network access: the required service and capacity are available over a vast network, and are accessed using standardised mechanisms to client platforms and devices
- Resource pooling: resources of service providers are shared by multiple clients using a multi-tenant model, with resources assigned to every client dynamically according to the level of use of each client
- Rapid elasticity: resources and services can be elastically provisioned and released so that other clients can have the released resources reassigned to them. The available resources are seemingly unlimited in the clients' point of view as a result
- Measured service: all volumes of resource and service used by a client are 'metered', and clients are billed according to metered usage. The metered usage can be reported and monitored by clients

A conceptual diagram of Cloud computing is shown in the figure below:

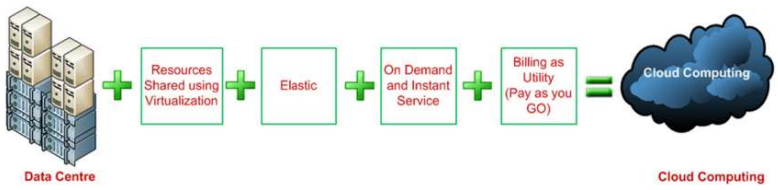


Figure 2.1 - Schematic definition of Cloud Computing (Source: Khorshed, Ali and Wasimi 2012)

A discussion on the typical Cloud typologies is shown in Appendix C.

2.5 Cloud Computing as a Tool to Harness IT Resources

Today emerging companies do not need to have a full-scale IT infrastructure and software installation in-house, as cloud service providers have different types of business packages to suit every stage of the business (Baun et al. 2011). As the company grows, so does the scale of use of the cloud service. The pay-as-a-service model of cloud service attracts IT Managers of SMEs and large corporations.

By migrating their internal IT infrastructure entirely or partly to a public cloud, private cloud, or a hybrid cloud model to cloud service providers, companies can save costs in the investment of internal systems infrastructure, and to reduce IT support staff numbers (Busch et al. 2014).

A pay-as-you-go cloud computing service also means companies can harness the IT resources in a much easier way. For example, without any complicated IT jargon, a business user can now go to a resource management console provided by a cloud service provider to inspect the status of cloud services (Baun, Kunze, Nimis & Tai 2011). Available resources in Cloud technology, such as CPUs, memory and disk usage, operating system type as well as user licenses, can be tracked online. Through the same console, the business users can also change the maximum capacity of system parameters, and provide an estimation of how much is going to be charged for the level of cloud services selected (Baun et al. 2011).

Most major cloud service providers have a set of tools to enable clients to control the cloud resources, without the need to highly train cloud computing specialists. Amazon Elastic Compute Cloud (Amazon EC2) from Amazon Web Service (AWS), a secure cloud services platform which offers different types of cloud services, is an example of a cloud service provider providing various tools to help clients acquire and control cloud resources for secure and scalable enterprise applications. Details of the Amazon Elastic Compute Cloud is described in Appendix C.

2.6 Security Issues in Cloud Computing

With all the advantages of cloud computing discussed above, the trend is widespread and continues to grow in the adoption of cloud computing among companies. Gartner Group (Stanford 2016) says by 2020, sales and deployment of computing services via IaaS and PaaS cloud providers will overtake enterprise data centres (Stanford 2016). As quoted from Gartner - in 2020 “a corporate ‘No-Cloud’ policy will be as rare as a ‘No-Internet’ policy is today” (Stanford 2016).

However, the transition of computing infrastructure and services from in-house to cloud-based generates concerns of security threats in participating companies (Fernandes et al. 2014). Unisys held a survey in 2016 showed that privacy concerns on storing personal biometrics information in the Cloud constituted 74% among all significant roadblock to incorporating biometrics into wearable technology (Unisys 2016).

On accessing the challenges of security risks in Cloud computing, Sendi & Cheriet (2014) mentioned CIA Triad model as a method to access the risks from cloud service providers in the three essential

aspects of information security. The CIA Triad model represents three categories of threats to information: confidentiality, which regards to unauthorised information release; integrity regards to the unauthorised information modification; and availability considers the unauthorised denial of use of information (Cherdantseva and Hilton 2013). An illustration of CIA Triad model is shown below.

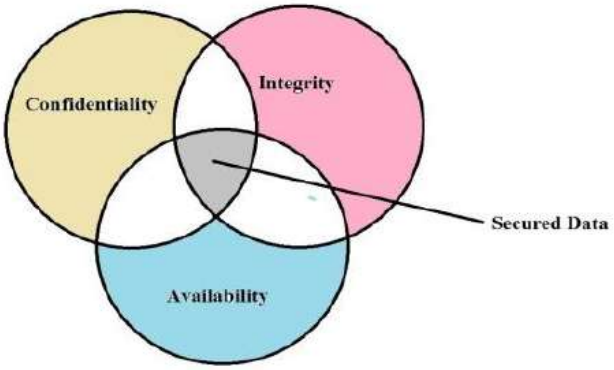


Figure 2.2 – CIA Triad Model (Source: Mohanty, Ganguly and Pattnaik 2018)

One can use the CIA Triad model to calculate the risk level as well as the value of the information asset based on the coefficients of the goals of information: confidentiality, integrity, and availability (Sendi & Cheriet 2014). There are other models for the measurement of information security, like McCumber's Cube and Business Model for Information Security (BMIS) (Cherdantseva and Hilton 2013). Below is a list of in-depth analysis of potential security threats in cloud computing environment.

The primary security concern in cloud computing is the threat of ***undesired data disclosure to unauthorised systems or personnel*** (Lokhande and Shelke 2013). As the data is stored in somewhere in the cloud infrastructure, unencrypted data and metadata, which stores the activities of the information access of companies, may be exposed to cyber attacks. Cloud service providers need to take all measures to ensure the information within their cloud infrastructure is adequately protected. The data also needs to be protected using some form of cryptographic protection mechanisms (Lokhande and Shelke 2013). A security mechanism, safeguard method and certification method is also necessary to protect the data and when data relocate (Tiwari and Joshi 2015).

The threat of data loss or leakage, on the other hand, can occur when cloud resources are shared with the same service provider. As one company disposes of a resource, it becomes a free resource which can be dynamically reused and reassigned. If the data deletion mechanism within the service provider is not appropriately handled, potential un-erased data of a company on released cloud resources may be reassigned to another company, which uses the same type of cloud resources (Lokhande and Shelke 2013). The security threat worsens when a data redundancy approach is adopted by a service provider to improve the availability of data or services (Jamil and Zaki 2011). Cloud service providers need to provide assurance to clients on a complete data disposal mechanism to ensure data in unallocated resources are 'erased' properly before it can be reassigned to another party (Jamil and Zaki 2011).

Another type of significant cloud security threat is ***unauthorised access control***, especially when applications and data are hosted in a public cloud, as the cloud resources are shared among multiple companies (Lokhande and Shelke 2013). This type of threats has broader implications, as a breach of an application in a hosted cloud service of a client will affect all other clients in the same cloud service. It could also result in the breach of other applications that use the same pool of resources in that cloud (Lokhande and Shelke 2013). A particular type of cloud service, named identity and access as a service (IDaaS, ACaaS), is created to provide expertise in dealing with access control in the cloud. IDaas and ACaaS will be discussed in the latter part of the thesis.

Interruption of availability is also an important type of security threat in cloud computing. As the processing load of service is distributed in the cloud infrastructure, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks would result in both degraded availabilities. It may also cause a potentially hefty bill on the client, as the client may still be liable to bear the cost in this pay-per-use model of cloud computing (Lokhande and Shelke 2013). Recently the 2016 Census website of Australian Bureau of Statistics (ABS) was crashed due to four waves of DDoS attacks on the 8th August 2016. The Census website was shut down for days to protect data collected before the outage that evening (Duckett 2016). Cloud service providers must put in enough counter-DDoS attack measures, such as geographically distributed data and services as well as simulated DDoS attack testing (Tiwari and Joshi 2015), to ensure the maximum availability of cloud services to clients.

Loss of governance application and data of a company happens when the client pass on the control of the company's application as well as business data to the cloud service provider (Jamil and Zaki 2011). As the client cannot pre-determine where the data is located physically within the cloud service, it would be hard for them to perform forensic investigations and audit trail of the location of data if needed (Lokhande and Shelke 2013).

Compliance with specific laws and regulations in countries is also a follow-on cloud security thread from the loss of control of applications and data of clients. Most cloud providers are multi-national companies, such as Amazon, IBM, Google, with uncleared physical boundaries of cloud resources. It then may not easy for the cloud customer to efficiently check the data handling practices of the cloud provider, and to make sure that the data of the organisation is handled in a lawful way (Jamil and Zaki 2011). In certain situations, clients want to know detailed information about where data is stored, as a requirement from countries where companies are registered for legal compliance requirements. Once information crosses national borders, it is hard to protect the data because of the rules and regulations of data protection change according to national judiciary laws (Tiwari and Joshi 2015).

As computing services are provided by external cloud service providers, they need to take enormous efforts to ensure their services are protected from security threats, to provide an uninterrupted service with data secure entirely from hackers in the large.

After examining different aspects of cloud computing, one would like to concentrate on several cloud services related to identity and access management (IAM), which is needed in the introduction of Cloud Passports.

2.7 Identity and Access Management, IDaaS and ACaaS

As the need for specialised services grows for corporations, different kinds of cloud services are introduced to cater for the increased need of various types of pay-as-you-go services. The two crucial cloud services to address this issue directly are Identification as a Service (IDaaS) (Thakkar 2013) and Access Control as a Service (ACaaS) (Wu et al. 2013). In fact, the access control management is usually embedded within IDaaS (Thakkar 2013).

In the traditional Identity and Access Management (IAM) model, when a person seeks access to a system (for instance, getting money from an ATM), the person needs to put in an identity claim (a key card), as well as security information to claim their identity (a password). The IAM system then uses the information presented and validates the person's identity from its back-office database and then finds out whether the claim of identity is valid or not (Witty at al. 2003). A diagram to show the relationship between identification and access rights verification is shown in figure 2.3:

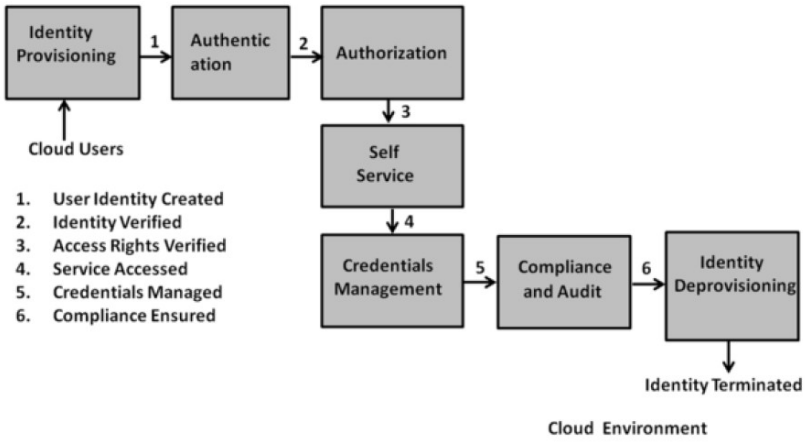


Figure 2.3 – Identity lifecycle management in the cloud (Thomas and Chandrasekaran 2016)

IDaaS is a cloud-based, pay-as-you-go service to authenticate a person against the identity s/he claims to be. In IDaaS, the cloud-based IAM, the software and database are stored in the cloud instead. Therefore, the validation process can be used on-demand, and the availability of the identity validation service is high and not restricted to geographical locations. Other functions of IAM like Single Sign-On, Federated Identity Management and Password management are all integrated into cloud-based IDaaS as well (Carter 2013).

ACaaS is a subscription-based service in a cloud environment to manage and validate the rights of a person to access the subsequent service requested (Wu et al. 2013). As there are different levels of assurance (or trust) required for a particular type of service, the access control management could be a complicated hierarchical structure. The concept of role-based access control models is added to ACaaS, in which users are assigned roles instead of individual access levels, and the level access permissions are assigned to roles instead (Wu et al. 2013). IDaaS and ACaaS are in a close relationship, which works as an authentication service chain providing authentication for a user.

2.8 Introduction of Biometric Authentication

Biometric authentication is a method of identification through behavioural or physiological characteristics (Unar, Seng and Abbasi 2014). Physiological characteristics such as the face, fingerprint, iris, and ear shape as well as behavioural characteristics such as gait, typing rhythm, voice and signatures could be used for biometric information (Unar, Seng and Abbasi 2014). As biometric characteristics captured should be unique and temporally invariant to each, the renewal of biometric capture of a person varies with the age of the person. In Australia, citizens over 16 years old can have a 10-year biometric passport, whereas children under 16 years old can only have a 5-year passport (Children's passports - Australian Passport Act 2005). Figure 2.4 shows the primary process of a biometric authentication system.

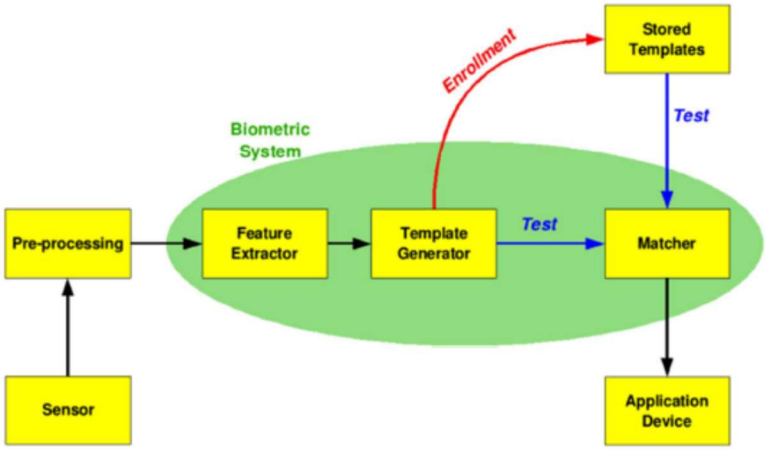


Figure 2.4 – A basic block diagram of a Biometric System (Vallabhu and Satyanarayana 2012)

There are two stages of processing for biometric identification systems (Unar, Seng and Abbasi 2014):

- Enrolment stage:
  - The person's ID is known, and his/her biometrics information is captured by a sensor, then processed and encrypted into an electronic template.
  - The template is stored in a secure and centralised database as an ID record of that person.
- Verification (or Identification) stage:
  - A sensor captures the person's biometric characteristics.
  - The information is then processed and encrypted into an electronic template in the enrolment stage.
  - A matcher takes these features and compares them to an existing template in the enrolment database.
  - A result will then be shown as to whether the person's captured biometrics template has a 1-to-1 match with the enroled template, and the ID of the individual is verified or not (identification will be a one-to-many search instead).

There are two types of authentication in a biometrics system: identification and verification. In biometric identification, a typical one-to-many database search is crucial and needed (Schouten and Jacobs 2009). A biometric template of the subject to be identified is generated by the biometric system, and then compared against a collection of existing biometric templates in a database - this usually takes a longer than verification (Jain et al. 2007). Verification, on the other hand, differs from biometric identification, as it does not necessarily require a database search to match the presented biometric trait (Schouten and Jacobs 2009). A user claims an identity by comparing the captured biometric data with his/her biometric template(s) stored in the system database (Jain et al. 2007).

2.9 Concept of Biometrics Identification as a Service (BaaS)

The idea of a Biometrics Identity and Access Management as a Service (BaaS in short) (Rose 2016) is illustrated in figure 2.5. The BaaS model is composed of the following components (Albahdal 2015):

- Biometric information capture and template generation
- Identity-as-a-Service - a cloud-based identity validation service
- Access-Control-as-a-Service - a cloud-based access control management service

An overall concept of BaaS is shown in figure 2.5:

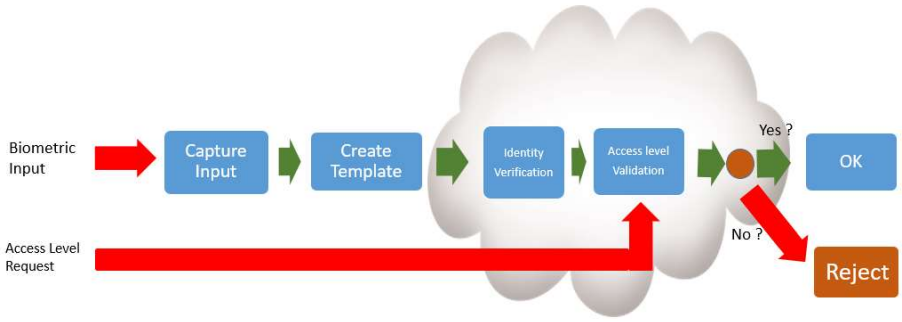


Figure 2.5 - Biometrics Based Identity and Access Management System (BaaS) – based on the description of BioAaaS (Albahdal 2015)

In short, a BaaS system is equal to an Identity and Access Management (IAM) system in the cloud, with the addition of using a person's biometric characteristics to validate against their enrolled biometrics template stored in the cloud, instead of using the traditional ID and password mechanism (Albahdal 2015). Using some form of ID and a password can be hard to remember, easy to forget and prone to attack by hackers (Ferbrache 2016). Biometrics information of the person him/herself, such as fingerprints, and facial information in the case of Cloud Passport, replaces the traditional passwords and become the key to service.

The differences between a standard Biometric ID authentication system versus BaaS is that the hardware and software of the ID authentication system are located somewhere in a physical location instead, whereas the BaaS system software and data are stored in the Cloud (Albahdal 2015). The cloud-based

ID system is then made available by the cloud service provider, without limitation in geographic locations. As the service is cloud-based, BaaS is scalable, and the service is charged on demand and by subscription.

Improved customer experience can also be achieved by implementing BaaS instead of the traditional ID and password system (Goode 2014). Apple pay - an initiative from Apple, enables iPhone users to make a better payment user experience by using fingerprints as the way to authenticate the person. On the other hand, banks need to catch up with the technology and provide some form of financial technology (FinTech) to attract customers to keep banking with them (Locke 2016). With the recent launch of using a "selfie pay" and a fingerprint to verify the identity to approve electronic payments by MasterCard (Locke 2016), the use of Biometrics instead of passwords for authentication is going to be more popular in the commercial world. Also, along with the enhancement of the encryption methods as well as cloud technologies, the idea of a global cloud passport system could be a reality in the not-so-distant future.

2.10 A proposed Cloud Passport model

Based on the information listed in this paper, a list of criteria for the establishment of a cloud passport environment is listed:

- A universal identifiable ID for each traveller:
    - The identifier can be the country code + Passport ID of the traveller, which can be constructed to be a unique ID
- An automated border control system for participating countries
- Biometrics information (Face) for the travellers is already enrolled in issuing countries.
    - The facial biometrics templates are readily available for all ICAO compliant e-passports already
- An acceptable security level of Identify Access Management in the Cloud (IDaaS)
- A robust globally secure internet communication link for participating countries
    - The communication channel allows countries to send and receive data online and on demand

In response to the concerns of the level of security of data storage in Cloud environment, the proposed model for Cloud Passport is configured to have the Biometrics database stored at the back-office of the corresponding countries, instead of storing the entire Biometrics database in the cloud. Biometrics information of the travellers is encrypted and sent from one country to another by a cloud-based secure information exchange channel. Microsoft Azure AppFabric Service Bus, as an example, is one of the services that connect to on-premise databases and applications (Suren 2010); it provides secure messaging and connectivity capabilities that enable distributed and disconnected applications in the cloud (Chou 2011). The flow of information between on-premise applications using the AppFabric Service Bus is shown in figure 2.6.

In the current Cloud Passport proposal (figure 2.7), the originating and destination countries send and receive validation information through a secure information exchange channel across the internet, to

exchange authentication information of travellers from their corresponding countries. This type of authentication configuration is chosen instead of an entirely cloud-based solution, in order to respond to limitations in privacy law, and restrictions on data retention of each participating country. According to Lynch and Bennett (2015), the critical issues of having a national biometric database for passport holders are "obvious security, political and privacy concerns, which would be extraordinarily difficult to overcome". By storing the data within the issuing country, concern over the security of Biometric data in the cloud can be minimised.

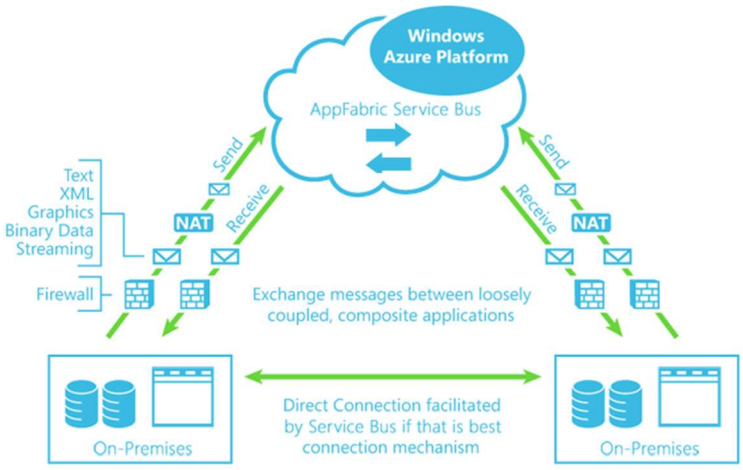


Figure 2.6 –Windows Azure AppFabric Service Bus, the link between on-premises service and cloud (source: Suren 2010)

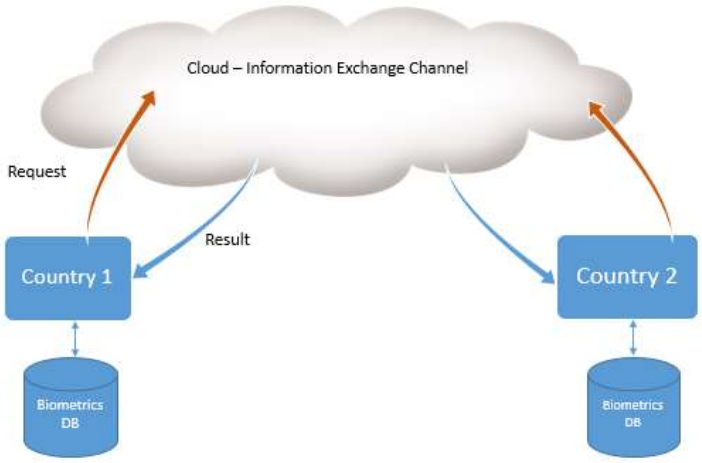


Figure 2.7 – Cloud Passport Information Exchange Channel for Authentication

The steps on how a Cloud Passport system works are highlighted as follows:

- At the Enrolment stage:

- The passenger provides one or more forms of biometric data to his/her originating country (in Australia, face and fingerprint is used for validation)

- The data will then be converted to electronic template data and stored in a biometric database in the back-office of the originating country

- The passenger also needs to nominate a particular kind of identification reference for themselves, to help search for the person's biometric record in the database (for example first and last name, mobile number and a phrase)

- A unique global passport ID is created, and along with the biometrics record and the nominated identification reference, is stored against the traveller's passport ID entry

- At the Verification stage:

  - Passengers present themselves to the counter (or an Automatic Border Control gate)

  - Passengers provide a particular kind of information for searching the biometric database of the originating country, such as country of origin, and nominated identification reference as provided before (first and last name as an example)

  - Biometric characteristics (face and fingerprints) of the traveller are captured, encrypted and converted to an electronic template for verification

  - The encrypted Biometric template data of the traveller, together with the nominated identification reference, is sent to the Cloud BaaS service for verification

  - The BaaS service will then supply the traveller's Biometric template, together with the traveller's nominated identification reference, to the traveller's originating country to search for the corresponding record in the originating country's Biometric database for verification.

  - Once the passenger is positively identified, the BaaS system will then check the passenger's record in the originating (or destination country, depending on the visa arrangement between the two countries), to validate their credentials (e.g. visa status and whether the traveller is on an exclusion list or not). All passport and visa information of the traveller can then be accessed once the traveller's identification is verified.

  - After verification, the BaaS supplies a message to the passenger on the outcome of the verification and informs the passenger to move on (if OK), or go to another gate for manual processing (if not OK).

2.11 Advantage and Challenges of Cloud Passport

A Cloud Passport inherits all the advantages of the proposed virtual passport, such as faster processing time, better facial recognition technique, minimising the reliance of physical passport to name a few advantages (Lynch and Bennett 2015). In addition to the points above, the cloud passport model tackles the shortcomings from the original idea of a virtual passport. As validation of the traveller is done on demand and online via a cloud-based communication channel, there is no need to "opt-in" and enter the full itinerary before the start of travel. Cloud passport validation systems can also adapt to ad-hoc changes to itinerary plans. As biometric authentication methods are used to improve user-friendliness, this should lead to better user experience (Goode 2014) and hence a better adoption rate of a cloud passport when introduced.

On the other hand, security of biometric information in the cloud becomes the primary challenge in implementing cloud passports. Since biometric information is personal and unchangeable in nature, as the biometric data and validation processes are performed in the cloud, there is a threat of breaching the privacy of a person if the biometric information has fallen into the wrong hands. A lot of research and development has been made in the area of encryption of raw biometric data, to provide an improved level of security when handling biometric data. A full cloud passport solution that is with a biometric database and service located in the cloud will only be widely considered once there is a way to adequately address the concerns of security and privacy (Hon and Millard 2013). In order to invite more countries to embrace the cloud passport model, the option of storing biometric information in the cloud is not considered at this stage.

2.12 Potential Development of Cloud Passport in the future

Currently, the arrangement of the Cloud Passport model is just for Australians and New Zealanders who travel between the two countries only. According to the vision by Julie Bishop (Quinn 2015), the next logical step is to introduce the Cloud Passport system to other countries that have similar border control systems and invite them to join in the Cloud Passport model. Countries that currently have similar ABC hardware and systems for border control are Canada, China, France, Hong Kong, Ireland, Japan, South Korea, Macao, New Zealand, Singapore, Sweden, Switzerland, UK and USA (Arrivals SmartGate, Department of Immigration and Border Protection 2016).

On the other hand, the *International Civil Aviation Organization* (ICAO) introduced a Public Key Directory (PKD) - a central platform for the authentication of e-Passports through the exchange of certificates and certificate revocation lists between participating countries on the internet (Hartmann & Körting 2009). As the secure data transmission link has been established between countries and the ICAO for the exchange of information for the PKD, ICAO should act as a hub to provide a centralised identity authentication service for participating countries, if the countries opt-in to exchange biometric information via secure links. Currently, the following states that participate in the ICAO PKD platform are Australia, Canada, France, Germany, India, Kazakhstan, New Zealand, Nigeria, Peoples Republic of China, Singapore, United Kingdom, United States, Japan, Switzerland and South Korea. If all countries listed above embrace the cloud passport system, then nearly two-thirds of people in the world will be able to travel to participating countries without a physical passport.

Another potential benefit of implementing a global Cloud Passport is that one can analyse the movements of travellers. The system can detect any abnormal activity for the prevention of possible crime or terrorist attack. The way to achieve this is listed as follows:

- All participating countries provide an audit trail of the history of departures and destinations of travellers. The information can then be collected in a central database, located securely in the cloud for access by participating countries
- For people with more than one passport, the cloud service can potentially merge travel history information together based on biometric identification; this will provide a better understanding of the full itinerary of the traveller's movements

By performing an analysis of the data collected in the cloud-based database, the combined full itineraries of travellers can be used to detect abnormal travel movements. Early detection of abnormal movement of suspects leads to prevention of potential terrorist attack.

2.13 Technology Acceptance Model and Unified Theory of Acceptance and Use of Technology

Most of the people agree on the potential benefits of the adopting new technology. However, there is a low level of acceptance and use of software measures in practice (Wallace and Sheetz 2014). In order to improve the level of acceptance of embracing new technology, an adequate model is needed to measure and predict the likely outcome of the use of the system (Legris et al. 2003). Two common technology adoption models, Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) are discussed in the following paragraphs.

According to Wallace and Sheetz (2014), TAM is used "to explain why individuals choose to adopt or not adopt a particular technology when performing a task". The origin of TAM can be backtracked to the theory of reasoned action (TRA), a model in the field of social psychology to explain how intentions of a group of people relate to their behaviours (Rauniar et al. 2014).

There are two aspects of intentions that affect the behaviour of people. Firstly, the attitudes of an individual which subsequently leads to influences of one's behaviour. Fishbein and Ajzen (1975) stated that the attitudes of an individual lead towards one's own behaviour and subjective norms to the world. On the other aspect, a set of beliefs or social norms that influence some individuals or a particular group of people on the behaviour (Rauniar et al. 2014).

TAM adopts the concepts of TRA on attitude construct by specifying the concepts of perceived usefulness (PU) and perceived ease of use (EU), in order to explain the behaviour for computer usage (Rauniar et al. 2014). A diagram to show the building blocks of TAM is shown below.

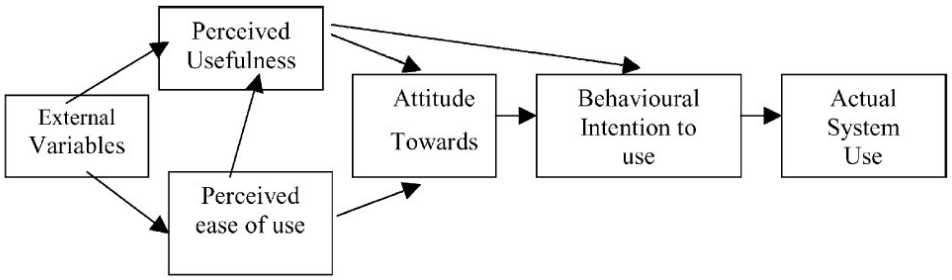


Figure 2.8 - TAM Model (Source: Legris et al. 2003)

One of the main benefits of using TAM is to allow users to trace the impact of a technology implementation from a set of external variables relates to attributes of intentions, internal beliefs and attitudes to the target group. TAM then measures the level of perceived ease of use (EU) and perceived usefulness (PU), and figure out a probability intention the use of a new system as an indicator of measurement of the satisfaction level of implementation of new technology (Legris et al. 2003).

There are similar models developed since the inception of TAM. Venkatesh el at (2003) has made efforts to combine eight different technology adoption models and formulate the Unified Theory of Acceptance and Use of Technology (UTAUT), with respect to understanding the acceptance of new information technologies. UTAUT brings different views on user and innovation acceptance together for the measurement of user acceptance of technology (Williams et al. 2015). A diagram of UTAUT is shown below.

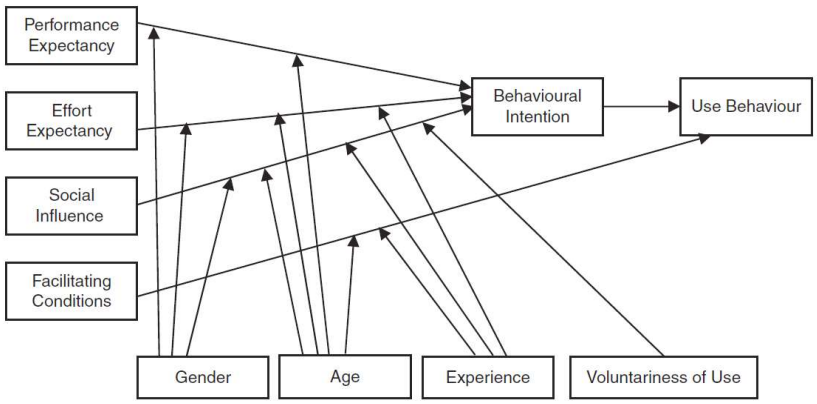


Figure 2.9 - UTAUT Model (Source: Venkatesh et al. 2003)

There are four direct determinants of UTAUT: performance expectancy, effort expectancy, social influence and facilitating conditions. These determinants, together with the influences by the parameters on gender, age, experience, and voluntariness of use, form the behavioural intention and ultimately the behaviour of the user towards a new technology implementation. Researchers can base a UTAUT model to identify key influence factors on the level of acceptance of information science projects. (Williams et al. 2015).

By Studying the above two models, one can adopt the concepts from the models above and construct a suitable model for the current research exercise on the acceptance level of Cloud passport.

2.14 Summary

In this chapter, the details of an Australian government proposal for a 'Cloud Passport' (Virtual Passport as a more precise name) are described in detail. The pros and cons of the idea of Virtual Passport in an operational perspective were examined, and see how shortcomings can be mitigated by the concept of a Cloud Passport system.

Different types of Cloud Computing models, as well as the concept of pay-as-you-go Cloud Services, are then discussed. The advantage on how companies can take advantage of the Cloud service model to harness IT resources is then listed in detail, along with a brief description of some major security issues that need to be addressed in Cloud Computing.

The detail of a modified version of Cloud Passport model is then discussed, with a brief description of the Biometrics cloud identity management service (BaaS) (Rose 2016). The challenges of implementing a Cloud Passport system among potential participating countries are then discussed. Finally, the thesis talks about future developments about how to exploit the Cloud Passport platform for better border control and prevention of potential terrorist attack, as well as a potential subscription-based cloud service for identity verification in financial sectors, and in other business environments.

With the blessing of the Australia government, hopefully, a user-friendly Cloud Passport system for Australian travellers can be realised in the not-so-distant future.

Chapter 3 - Research Philosophy

3.1 Introduction

In Chapter 2 of the thesis, the details of the proposal of Cloud Passport was discussed, as well as the drivers and the barriers to the implementation of the electronic version of a travel document for Australia. The research question and research objectives are also stated in Chapter 1 based on the literature review on the Cloud Passport. To answer these research questions, one needs to develop a valid research methodology that is backed up by certain underlying research philosophies. The ultimate objective of the research is to obtain results to the research questions and create new knowledge in the process. Let us examine some underlying research philosophies for the research question.

The research question is restated as follows:

> *RQ 1: Given the current level of technology that enables a Cloud Passport model - what are the opinions of select members of the Australian general public to the adoption of a cloud passport?*
>
> > *RQ 1a: What are the concerns of a sample of Australian with regard to replacing the current physical passport with a digital version?*

The research objectives are to obtain answers to the research questions and to report on findings on the attitudes of a sample of Australian on the vision of Cloud passport as an alternative for the current travel document arrangement. This chapter starts considering the building blocks to develop research philosophies. It then compares different types of research philosophies, and then to choose mixed research methods in response to the nature of the research topic. Finally, a model of the drivers and barriers to the adoption of Cloud Passport by Australians was proposed.

3.2 Discussion of Research Philosophy

The formation of research paradigms used for the research is closely related to the underlying research philosophy for the research topic. Therefore, it is important to examine different types of research paradigms and their underlining philosophies, so that the most suitable one for the research topic shall be chosen in order to have the right answers for the research question.

Research philosophy is a set of assumptions that guide how the world is viewed (ontology), and inference the way on a particular view of the relationship between knowledge (epistemology), and the process by which it is developed (methodology) (Anderson 2013). The assumptions in a selected research philosophy become the basis of the research strategy and method for the research (Saunders et al. 2015). A research paradigm, on the other hand, is a set of belief and agreements, which are universally accepted among scientists, providing an approach to understand and seek a solution to a research question (Kuhn

1962). Typical research paradigms are Positivism, Interpretivism (or Constructivism), Criticism and Pragmatism (Anderson 2013).

Positivism describes the world as a stable state, in which all measurements of research subject can be obtained from an objective way, without affecting the phenomena being observed (Levin 1994). Positivism is based on scientific experience, which is both verifiable and repeatable (Srivastava 2001). Results obtained from Positivism are reliable as one can expect the same result when he or she measures the research subject at different times and with different researchers; the result is also valid, as the results are measured in order to answer the research question (Anderson 2013). The set of assumptions in the view of positivism can be summarised as follows. Positivism assumes the world as an objective reality that can be understood, and the world is governed by certain universal laws (Anderson 2013). On the view of epistemology, knowledge can be derived from measurable scientific methodologies (Anderson 2013). Common research methods for positivism are laboratory experiments and surveys, with an emphasis on quantitative information (Recker 2012).

On the Positivist view of the research process, Raddon (2010) state that it starts with a theory or a model, which needs to be confirmed and verified through a core research question. The research method is then designed based on the model, and data collected for the designed method. The data is then analysed and interpreted, and the findings of the original model are then compared (Raddon 2010).

Interpretivism argues the world is too complex; it cannot be described by certain laws and theories like researchers in physical sciences (Saunders et al. 2015). A subjective way to interpret the viewpoints of observers is the preferred way to study the social order (Bhattacherjee 2012). Researchers need to consider differences between humans as observers in their view to the world and have empathy to understand the world in their perspective (Saunders et al. 2015). The set of assumptions for interpretivism is summarised as follows. On the view of ontology, interpretivism thinks the world cannot be view as a single truth, but by subjective viewpoints of different observers (Saunders et al. 2015). On the view of epistemology, knowledge is obtained by subjective interpretation of observers, in order to have a better understanding of the world (Bhattacherjee 2012). Standard research methods for interpretivism are narratives, interviews, observations, ethnography, case study, with an emphasis to obtain qualitative information (Anderson 2013).

The interpretivist view of the research process, an initial model, may also have proposed for verification through the research method for the model. However, inductive reasoning is emphasised as the research tries to establish or redefine a new theory based on the data gathered through qualitative techniques (Raddon 2010). Grounded theory, which can be interpreted as a “bottom-up” approach, is a typical approach in qualitative research, and it is highly related to interpretivism (Lodico et al. 2010). Apart from the above the two research philosophies, let us discuss Criticism and Pragmatism briefly.

Criticism views that the reality can be apprehended, which can be shaped by social, political, cultural, economic, ethnic and gender-based factors (Guba & Lincoln 1994). An aim of the critical research is to challenge the status quo (Ponterotto 2005). By carrying out critical research on the topic, the reality will

inevitably be influenced by the research (Guba & Lincoln 1994). This is, in contrast, entirely different from the theory of positivism (Ponterotto 2005).

Lastly, Pragmatism recognises that choosing a paradigm for certain situations is not realistic in practice (Saunders et al. 2015). In order to get answers to the research question, pragmatists will use any method that works (Lodico et al. 2010). Usually, a mixture of research paradigms is employed for practical research. In the following paragraphs, conventional research paradigms for Information Systems research will be explored in detail.

3.3 Comparison between Positivism and Interpretivism for Information Systems Research

According to Galliers (1991), the two dominant research paradigms for scientific studies in the western world are Positivism and Interpretivism. The discussion of the two dominant research paradigms are listed as follows.

There has been much debate on the preference of the research paradigm between Positivism and Interpretivism for Information System Research. As Information System is a study of mainly human and social related nature, it should be classified as social sciences rather than physical sciences (Hirschheim 1985).

The modern development of Positivism started from the twelfth century AD/CE when Greek philosophical writings were translated into Latin, though the development was limited due to influences from the Church authorities. A breakthrough started when a great awakening occurred in Europe in the sixteenth and early seventeenth centuries when the authority of the Church was challenged by different parties (Hirschheim 1985). As a result, scientific ideas would no longer be constrained by the Church and led to the accelerated development of the theory of positivism (Hirschheim 1985).

Anti-Positivism, also known as Interpretivism, started to develop in the nineteenth century when a group of researchers broke out and proposed that there was a need for something other than Positivism research philosophy (Hirschheim 1985). While the method of Positivism concentrated solely on physical or social rules, it failed to address the fundamental experience of life, as each individual needed to be understood based on their culture as well as the social life they are in (Hirschheim 1985).

Burrell and Morgan (1979) stated that the Positivism practice approach has gradually caused more and more problematic issues, since researchers unavoidably put in their values with the frame of reference for the research area, and this affected the outcome of the study. Moreover, in the field of social science, as each subject in the research has one's own "essential spiritual character" (Burrell and Morgan 1979), the subject as a human, as a free spirit, could not be objectively studied and establish a law upon, but should be explored by a philosophy of speculative methods (Burrell and Morgan 1979).

Over the years, it has been drawn to a conclusion by social science researchers that simple scientific method, while it is suitable for researchers in natural science, has limited the progress on the study of the behaviour of a human in social science research (Hirschheim 1985).

3.4 A Pragmatic Approach to Information Science Research

In the recent development of research approaches, the idea of Post-Positivism has emerged as an alternative approach for social science research, as some scholars claim that the traditional research philosophies are not suitable for the research subjects (Hirschheim 1985). The aim of Post-Positivism is to move away from the habit of using solely Positivism, and introduced the term "methodological pluralism", which means that there are many methods other than a single method that can be utilized for social science research, as long as there are correct ones suitable for the research subject (Hirschheim 1985).

Saunders et al. (2015) also expressed that it is practically unrealistic to choose one method over another for social science research. He suggested taking a pragmatic approach when selecting the right methods for social science research, as the most crucial factor for research is to find the best research approach to explore and answer the research question. As long as the questions do not specify the use of particular research philosophy, it is entirely feasible to use one approach for a part of the research questions, while using another method for other areas of the research. The main aim is to get the best mix of approaches to answer the research question (Saunders et al. 2015). A pragmatist in social research should choose the most suitable research method to renegotiate, debate and interpret the research subject and solve the research question (Patel 2015).

Mixed Methods approach, as introduced in Creswell (2013), combines qualitative and quantitative strategies, either use both methods together or in different parts of researchers. Mixed Methods provide a way to take the strengths of both qualitative and quantitative strategies and use them cooperatively while keeping the uniqueness of each of the strategy to tackle the parts of sophisticated social science research (Recker 2013).

3.5 Mixed Method Research for the Research Topic

In chapter one, the discussion on the research objective was to determine the level of acceptance on the proposal of Cloud Passport by a sample of Australians. Given the subjects of the research are the Australian and assumed that Australian people might have different opinions on the research topic, one can conclude the current research topic falls into the area of social science research. That is, to study the differences between humans as observers in their view to the world and have empathy to understand the world in their perspective (Saunders et al. 2015). The outcome is within our expectation as most of our research falls into the social science research area (Hirschheim 1985).

The research topic can be breakdown into the following areas. Firstly, the research should collect demographic information of the sample group in order understand the composition of the Australians

who opinions on the research subject were sought, which can provide a better analysis on the opinion of different types of respondents. Secondly, the research should collect structured data on the primary parts in order to have a quantitive measurement on the degree of support for the implementation of cloud passport. Finally, the research should allow the respondents to give feedback on the research topic in a free text format so that they can express their opinion on the research without any restrictions. The research can then analyse the free-form text to get insights from the respondents which may not be able to be collected in the structured format.

In order to efficiently analyse the collected information, a Mixed Method Approach was adopted as the strategy for the research topic. The advantage of adopting a mixed method approach to the current research topic is listed as follows. Since both quantitative and qualitative methods of data collection may have their own advantages and constraints at the same time, the use of both methods can then shield off the disadvantages of another method, and strengthen the effectiveness of data collection for the research s a hold (Creswell et al. 2003). This is especially important on social science researchers, as one needs different kinds of methods to understand the complexities of social phenomena (Creswell et al. 2003).

The research area can be divided into two parts. The first part of research is to use a quantitative method to collect objective data on the composition of a sample of Australian being interviewed, as well as responses from the interviewee on the degree of support on the main parts for the implementation of cloud passport. The reason for using a quantitative method on the first two areas of research topic is because responses of the composition of the Australian general public, and the degree of support of the implementation of cloud passport is suitable to be categorised and quantified into numerical values, and make collected data easier for analysis and presentation of the research.

The type of questions for the quantitative part of the research approach can be categorised into two groups. In the first group of questions are to capture demographic information of the samples, such as state, age, gender, education level and employment status. This gives a better insight into the response to the questions of sample groups in different categories. The analysed result can provide a different level of acceptance of the research topic, in which remedial actions can then be formulated to address the concerns from that particular group of people. The second part of the questions for quantitative research approach is the core question which directly relates to the research topic. Questions list the acceptance of the concept of Cloud Passport, the opinion on the changes from a manual process which operated by a human, to an automated process which machine and new technologies are used instead. Quantified responses (from 1 to 10) are then captured, which can then be statistically summarised in a numerical format for comparison.

The last part of research is to use the qualitative method to gather feedback from interviewees for the research topic in an unstructured format a free-form text. The reason for using qualitative method for the last area of the research topic is to allow interviewees to express their opinion on the research topic freely, usually in a text format, so that one can capture the subjective view of all respondents and have a better understanding of the social and cultural phenomena of the research topic.

3.6 Drivers and barriers to the adoption of Cloud Passport

Chapters 1 and 2 discussed in detail the motivations for the idea of Cloud Passport model, as well as the advantages and challenges of the proposal of implementation of Cloud Passport in Australia. The current research topic belongs to an information science category, with the study relates to the interaction between human and the advancement of technology (Lee, 2001), and how new technologies affect organisations and society, both in a positive and a negative way.

The introduction of a carefully designed technology solution, with a detailed plan for delivering the new product or service, can initiate a favourable impact to an organisation and to the society (Avison and Fitzgerald, 1995). However, the introduction of technology to replace human workers may have a social and psychological impact on the people in the society. When Ford (2015) discussed the rise of robots, argued that the introduction of more robots to replace human workers will decrease the rate of job creation for human, with a more extended period of recovery of employment level after a recession, and a rising of numbers in long-term employment (Ford 2015).

Both positive and negative impact of an introduction of an Information System (IS) model needs to be studied, in order to have an adequate change management process for a successful implementation plan for the technology solution.

From the first two chapters of the thesis, one observed the main drivers for the adoption of Cloud Passport model. Firstly, there is an increased need for border control agencies of different countries to have a more efficient solution to cope with an ever-increasing volume of travellers passing at borders gates (IATA 2016, Roberts et al. 2014). Secondly, security checking systems with higher efficiency and a lower error rate is needed to handle an increased volume of the flow of travellers, and to improve security level against terrorist threats (White et al. 2015). Because of the above requirements, the Australian government needs a viable solution, with a scalable capability of resources to cope with the future growth of travellers for border control. The recent development of technologies in the last two decades makes a valid case for the proposal to implement Cloud Passport model among countries (Lynch & Bennett 2015).

Other the other hand, potential issues that may become barriers to the adoption of Cloud Passport model are as follows. Firstly, there are concerns on whether the level of security on the storage of personal data, especially biometrics data as they are hard to change, can prevent the loss of personal data to hackers (Nandakumar & Jain 2015). The vulnerability of cloud technologies, as well as the network security on the transmission links between countries, are also deterring countries from embracing the new technologies (Fernandes et al., 2014). Secondly, as there is a different level of stringentness of privacy concerns among countries, it's hard to get an agreement globally on the acceptance of the implementation of Cloud Passport globally (Bellman et al. 2004). The differences in the level of technology between countries to embrace the changes for the implementation of Cloud Passport. Apart from that, there is generally a mood of distrust of Australian government by some citizens in a country when some form of identification is introduced on the people in that country (Murphy 2017). Those people may think in a conspiracy theory that the government may use personal information to impose a particular kind of

control of the people. The multiple ill-fated attempts by the Australian government to introduce some form of a national identity card is a good example. The proposal to introduce the Australian Card in 1985 (Greenleaf 1987), and a repeated attempt of Access Card by John Howard after the London Bombings in 2005 (Jordan 2006) were both called off due to either technical reasons for Australian Card (Greenleaf 1988), or a change in Australian government for the Access Card (Stafford 2007). A call for a national identification card by the Abbott government (Osborne 2016), and criticisms to the introduction of cashless welfare card payment by the Turnbull government (Baxendale 2017) are just some of the repeated attempts and failures of introducing a national identification system by the Australian government. An adequate change management plan is needed by the Australian government to get the society ready to embrace new technologies.

3.7 A Proposed Research Model for the Adoption of Cloud Passport

As the drivers and potential barriers for the adoption of Cloud Passport model were identified, a high level IS model was created to describe the Cloud Passport and the related drivers and barriers at the beginning of the research. The model can be illustrated below in figure 3.1.

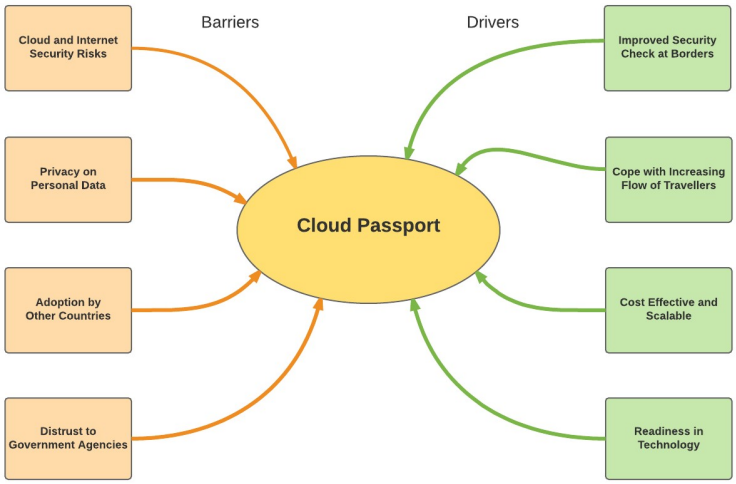


Figure 3.1 - A Proposed Cloud Passport Adoption Model

One of the aims of the research is to verify the Cloud Passport adoption model created from the initial investigation. Once the research data is collected and analysed, one then revisits the above model and find out for any “fits” and “gaps” between the original model and the findings from the research data. The Cloud Passport adoption model may need to be updated to reflect the social opinion from Australian people, which may help to create a plan for the implementation of Cloud Passport.

With a limit research timeframe and resources available, the aim this research will concentrate on collecting opinion of a sample of Australian, via convenience sampling, and provide a guide on the trend of the opinion of the research topic from a sample of Australian people. A more extensive and a better

representation of full Australian opinion may then be conducted in a future study based on the outcome of this research paper.

3.8 Conclusions

In this chapter, different types of research philosophies were discussed, with the concentration of a comparison between positivism and interpretivism. A pragmatic approach to the selection of various research paradigms led to the choice of mixed research methods in response to the nature of the research topic. The drivers and barriers to the adoption of Cloud Passport in Australia were then analysed and proposed a model of the drivers and barriers to the adoption of Cloud Passport by Australians.

In the following chapter, the methods and instruments for the research of acceptance of Cloud Passports will be examined in details.

Chapter 4 – Research Methodology

4.1 Introduction

The central theme of the thesis is to study the response of a sample of Australians to the proposal of a Cloud Passport, a cloud-based automated system allowing travellers to travel freely between countries with a higher level of security, free of fraud, and without the need of a physical passport. The Australian government has endorsed a potential implementation of a Cloud Passport (Lynch 2016). Talks were underway for a trans-Tasman agreement on the trial of the Cloud Passport (Bourke 2015).

The approach of the current research was to conduct a survey of a sample of Australians to assess the attitudes toward the idea of Cloud Passport. The questions in the survey tried ascertain how Australian thought about the idea of a paperless passenger identification system; to replace government personnel with automated border gates; to introduce biometric features (face, fingerprint, iris, etc.); to verify the identity of a traveller; and to store travellers' biometric features in a government database, which can be made available to other countries through a secure cloud-based communication link for identity authentication purposes. Based on data collected from the survey, the research reports an aspect of social phenomena of Australians on the perception of Cloud Passports, and provide recommendations for possible successful implementation of Cloud Passports.

The chapter will firstly describe the instruments chosen for data collection, based on the research method that was selected for the research topic. Secondly, the design of the questionnaire for the survey was discussed. The methods to collect survey data and the methods on how to process and analyse collected data were then evaluated. Finally, the plan to archive and delete the collected survey data will be reviewed.

4.2 Instruments for data collection

In the chapter on Research Philosophy, Mixed Method (Creswell 2013), a combination of Quantitative Research and Qualitative Research, was chosen to be used as the research approach. As the study is to determine the response of the Australian samples to the adoption of Cloud Passport, a survey method was chosen as the instrument for data collection.

Bhattacherjee (2012) notes survey research is a research method using standardised questionnaires "to collect data about people and their thoughts, and behaviours in a systematic manner" (p.73).

Recker (2013) lists the advantages and disadvantages of the survey method (p.77). On the benefits aspects, firstly surveys are easy to handle and can be coded and scored easily. Secondly, the values in the survey can be constructed to reflect the predicted results. Also, the responses in the survey can be used to generalise as to the whole population studied, or to other similar population size and mix. Once a survey is set up, it can be repeated in different time and places, to give comparable results on various scenarios. The result of a survey can predict the behaviour of the sample and can be used to test particular

propositions objectively. Finally, a survey quantifies the findings, which can help for a detail qualitative analysis.

Recker (2013) also listed the downside of the survey method (p.77). The survey method gives the behaviour of the target population at a particular place and time only. Assumptions for the survey conducted must be valid for a particular context as well. Secondly, surveys do not provide as rich or 'thick' description of a situation as a case study. Moreover, surveys do not provide substantial evidence for causality between surveyed constructs as a well-designed experiment. Finally, surveys are often susceptible to low response rates, which can diminish the generalisability of the results.

As the aim of the research is to obtain a holistic view of a sample of the general public on the adoption of Cloud Passport, the questions of the survey need to be structured so that the data collected can be analysed in an efficient way for the research topic. A questionnaire is then chosen as the instrument for data collection. The questionnaire of the survey is divided into the following sections or themes:

- A participant information and consent form
- A brief introduction to the Cloud Passport, and the nature of the survey
- Demographic information (gender, age range, education level & occupation type)
- Passport and travel-related information of the interviewees
- The degree of acceptance of the concept of Cloud Passport (travel to other countries without the need for a physical passport) as a future method
- Attitude toward machines, rather than people in border control
- The use of one or more biometric features (e.g. face, fingerprint and iris) to verify the identity of a traveller
- The degree of concern about having biometric information (face, fingerprints as examples) stored in the cloud as the identification method for Cloud Passports
- General open-ended comments

Based on the chosen research method, the questionnaire of the survey is constructed into two parts for data collection. Firstly, a quantitative approach is used for the first 16 questions of the questionnaire, to compare the level of acceptance of different aspects of Cloud Passport use. It is then followed by a qualitative approach to the 17th question of the questionnaire. By using a free-form text input field, the question can capture general ideas of the interviewees on the survey question. The data collected from the survey was then analysed both quantitatively and qualitatively, to determine reactions and trends of public opinion on Cloud Passport. Any gaps which are uncovered in the original Cloud Passport proposal will be highlighted in the discussion chapter of the thesis.

4.3 Survey questionnaire design

The survey questionnaire consisted of 17 questions, and the survey questions are constructed to be simple and direct questions, to be easy to understand for most adults over 18 years old. Most questions in the questionnaire are in structured response formats, checkboxes or 'circle and answer' responses or Likert scales (Surveymonkey 2017), which helps interviewee respond more efficiently, enabling summarization

of replies from the survey (Trochim 2006). A free-form text box is included as the last question at the end of the survey. The question allows participants a short textual response at the end of the survey for feedback purposes. Researchers can inspect this question to gain qualitative insights from an interviewee based on comments related to the survey.

The questionnaire was grouped into six categories. The first category of the questionnaire related to participant information and consent. The second category was an introduction of background information of Cloud Passport. It is then followed by questions on the demographic data of the interviewees, and then the passport and travel-related information of the respondents. Questions on the level of acceptance of the components of Cloud Passport was then listed out. Finally, a free-form text box was available for general comments on the survey topic. Details of each of the categories are covered in the following paragraphs.

Part 1 - Participant Information and Consent:

The questionnaire was preceded by a cover letter and participant information and consent form (PICF). The PICF includes an invitation to participate in the survey, a brief introduction to the survey, and a section describing the voluntary and private nature of the survey. Contact details of the investigator (Tonnie Lam) and the supervisor of the investigator (Dr Peter Busch) are provided as contacts for any questions of the survey. The ethical aspects of the survey have been approved by the Macquarie University Human Research Ethics Committee (HREC). Contact details of the Ethics Committee are also provided at the end of the PICF. Answering 'yes' to the PICF, participants confirm they are 18 years or older and give consent to participate in the survey.

A copy of the approval letter of the survey by the Macquarie University Human Research Ethics Committee (HREC) is attached in Appendix A.

Part 2 – Introduction of background information on Cloud Passport

An introduction to Cloud passport is provided at the front of the questionnaire to ensure interviewees have the necessary information to start the survey. The aim of the survey was stated at the beginning of the introduction, followed by a brief description of the components of Cloud Passport. The benefits of the proposed Cloud Passport implementation were then listed. Finally, the initial scope of the proposed implementation of Cloud Passport was then mentioned for the interviewees.

Part 3 – Demographic information of the interviewees

A list of demographic questions, such as the state of residence, age, gender, education level and work type is included in Question 2 to 6 of the questionnaire. Question 2 is the state of residence of respondents. The result will show the spread of interviewees across the states in Australia, and one can then verify the level of representation for an Australia-wide survey. Data collected from questions 3 to 6 on age, gender, education level and work type allow us to form a profile of different characteristics of interviewees for further data analysis purposes.

Part 4 – Passport and travel-related information of the interviewees

Questions 7 to 11 related to nature and the habits of overseas travel of respondents. Firstly, respondents were asked in question 7 and 8 whether they had a passport, and the country or region if they had one. Questions 9 to 11 sought to determine how frequently respondents travelled overseas, the nature of the trip (whether for business or leisure), and the regions interviewees travelled or planned to travel. A list of common country regions was provided for the interviewee to choose from.

Part 5 – Level of acceptance of the components of Cloud Passport

Questions 12 to 16 are the core questions to collect data on the degree of acceptance of the concept of Cloud Passport. The format of questions 12 to 15 was a Likert scale from 1 to 10, with 1 being least favourable, to 10 strongly favouring the question. These three questions tried to capture responses to the following statements from interviewees are, firstly, the attitude towards machines rather than people in border control. It then followed by a question on the use of one or more biometric features (such as the face, fingerprint and iris) to verify the identity of a traveller. The last question of the three questions was to ask for the degree of concern on having biometric information (face, fingerprints as examples) stored in the cloud as the identification method for Cloud Passport.

Question 16 of the survey is a simple "yes" or "no" question, seeking opinions from interviewees on whether Cloud Passport will be widely used in countries around the world in the next 10 – 20 years?

Part 6 - General comments on the survey topic

Question 17 is a free-form text box allowing interviewees optional comments. Responses to question 17 will be interpreted using lexical analysis software, in order to gain insights from respondents on the Cloud Passport.

4.4 Survey data collection method

Given limited time and budget on the research, the method of convenience sampling was adopted as the method to collect opinions from the Australian public. Convenience sampling is a sampling technique where people are chosen based on availability, close to hand or convenience, as people who are invited to participate in the survey are the ones who are easy to access in a designated public space (Bhattacherjee 2012). It does not have the full representation of the target group, but one can get an understanding of the opinion of a random sample of people on a particular topic.

The questionnaire of the research was in two formats: a paper-based version and an online survey form created in www.surveymonkey.com. The paper-based questionnaire would be used for the street survey. The collected data is then converted into electronic format for analysis and reporting purposes.

The online version of the survey is set up in surveymonkey.com, and the link to the online questionnaire is promoted by advertisement on the Facebook social network platform. The collected data from the online survey can then be downloaded for further analysis and consolidation of results.

The online survey method was chosen after an evaluation of the two types of survey data collection methods. The reasons for choosing are discussed below. Facebook is the most popular social network application for subscribed users in Australia, with 16 million registered users (Cowling 2017), in an Australian population of 23 million as of 2013 (Australian Bureau of Statistics 2017). A Study in the US (Wells & Links 2014) showed around 50% of the US internet population aged 13 – 19 used Facebook from a computer at home in a four-week period in March 2011. Similarly, the use of Facebook as the media to promote the survey is expected to be an efficient mechanism to gain attention from a sample of the general public in Australia. Secondly, the online survey can reach a wider audience by promotion through Facebook. As the target participants are from all states instead of from a local area, the data in the online survey can provide a better representation of the opinion of the whole of Australia (Harrison 2017). Moreover, the method of promotion via Facebook is non-intrusive by nature, as people choose to access the online survey by clicking on the Facebook advertisement. Lastly, as the advertisements in Facebook are inserted by a complicated ranking algorithm (Constine 2016), a possible probabilistic random sample of people to participate in the online survey can be achieved. As a consequence, all Australian Facebook users may have an equal likelihood of selection via the advertisement on their Facebook page.

The details on the setup of a Facebook advertising campaign for the survey is discussed in Appendix D.

The duration of the campaign had been set for 1 month, started from 1st February 2017 to 28th February 2017. Apart from the setting above, a rule had put in the campaign to the limit the number of advertisements to show during the campaign period. The survey result data is stored in the surveymonkey.com website, which can then be downloaded and used for analysis and reporting purposes.

4.5 Methods for processing and analysing data collected

Since the survey questions are constructed both quantitatively and qualitatively, different methods are used for the analysis of data gathered from the survey to determine reactions of the general public samples to the idea of Cloud Passports. The various methods for data processing and analysis are a univariate analysis of questions with structured response formats (Anderson et al. 2014); bivariate analysis of data from more than one question (Bhattacherjee 2012); and textual analysis of free-form text (NVivo 2017).

Univariate Analysis – or called single variable analysis, is to analyse general properties of one variable (Anderson et al. 2014). The typical properties for univariate analysis are frequency distribution, central tendency (mean, median and mode), and dispersion (standard deviation). Question 1 to 16 of the survey uses univariate analysis methods to produce tables and charts, as the questions are quantitative in nature.

Bivariate analysis - Bivariate analysis investigates how two variables relate (or correlates) when they are analysed together (Bhattacherjee 2012). In this survey, Excel was used to develop bivariate collated results between the data from two questions (acceptance level of Cloud Passport and by age group as an example) and then produce statistical reports and graphs to represent some potential insights of the relationship between questions in the questionnaire.

Textual analysis – or text analysis, is a method to organise and find insights from unstructured and qualitative data (NVivo 2017). In this survey, the free-form text data from question 17 will be analysed through the content analysis method, to gain insights of the interviewee on the idea of the implementation of Cloud Passport. Detail of the content analysis method for question 17 of the survey is shown below.

4.6 Using content analysis for qualitative method

According to Bengtsson (2016), the steps to perform analysis of textual data received from the survey are as follows. The first step, decontextualization, is to identify meaningful units within the raw text data and create a list of keywords for coding purpose. Then, recontextualization is to include essential content related to the research topic and to exclude inappropriate words. Often efforts are needed to compare the keywords with the original data to deduce the real meaning of the coded words. The third step, categorization, is to identify homogeneous groups among the coded words and try to bring the core subjects together. The last step, compilation, is to conclude the findings with references the coded words and the original texts in the survey. An overview of the qualitative content analysis process by Bengtsson (2016) is shown in figure 4.3.

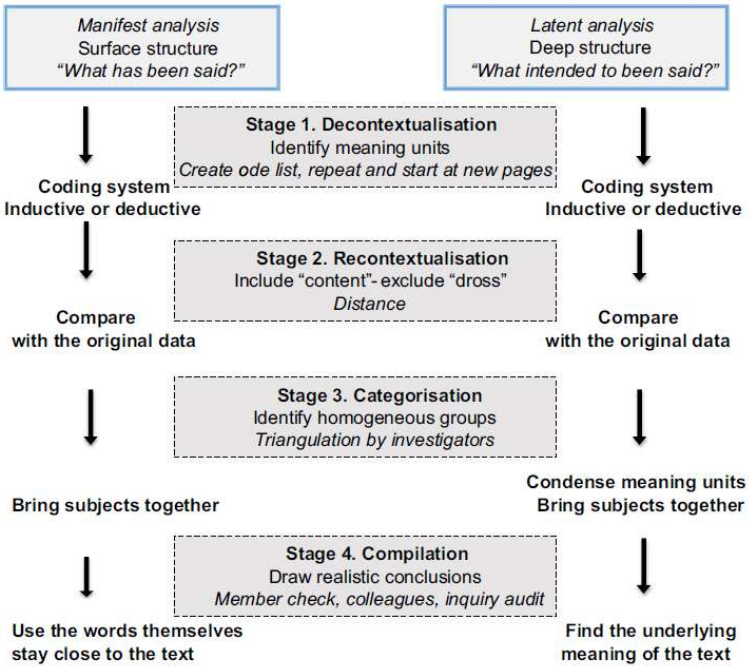


Figure 4.1 – Overview of the process of qualitative content analysis – Data Analysis

4.7 Archiving and removal of survey data

It is a requirement of the HREC of Macquarie University that a plan needs to be drawn on how to handle survey data collected. The plan needs to also fulfil the requirements of the Australian Code for the Responsible Conduct of Research (Australian Research Council 2007).

Below are the details as to how the survey data be handled during and after the research:

- *Formats of the data are stored in the research project* – the collected data will be stored as Excel data files.
- *How the data be stored in the project* – survey data files are to be stored in surveymonkey.com. A copy of data file is stored in Microsoft OneDrive in the cloud.
- *How the data can be stored after the project* – all data files will be moved from surveymonkey.com and from Microsoft OneDrive cloud drive to offline storage (USB drive or DVD-ROM).
- *How to ensure collected data is securely stored, to ensure the security of information from misuse, loss, or unauthorised access* – both surveymonkey.com and Microsoft OneDrive have passport-protected access mechanism to keep the collected survey data from unauthorised access. The data in offline storage will be encrypted and will store in a secure location to prevent from falling into the wrong hands.
- *The duration of storage of archived data* - the data is to be stored ten years for the potential use of further research in a similar area.
- *Reporting on the status of the archived data* – the status of the archived data will be reported to the Ethics Committee yearly.
- *The method to dispose of the data after the archiving period* - the data will be deleted from offsite storage (USB drive to be reformatted, DVD to be destroyed).

4.8 Summary

In this chapter, a survey was introduced as the instrument for the data collection on the idea of the adoption of Cloud Passport by a sample of Australians. The six categories of the questions were then discussed when designing the survey, followed by an analysis of the different method to collect data for the survey. After evaluation, the method of an online survey promoted by advertisements in Facebook was chosen. A brief discussion of analysing the data gathered using univariate analysis, bivariate analysis and content analysis of free-form texts were stated. Finally, the approach to archive collected data, as well as removal of archived data was then reviewed.

In the following two chapters, the quantitative and qualitative results from the data collected from the survey will be analysed in details.

Chapter 5 – Quantitative Result Analysis

5.1 Introduction

In this chapter, the quantitative analysis results of the data collected from the survey were elaborated. The primary emphasis on the analysis was on collected data from question 1 to 16. Bivariate analysis on data from a combination of two questions was then carried out, followed by a conclusion to state the observations from the survey results. The analysis of the survey results was presented in a plain and unbiased way.

A pilot run of the Facebook advertisement campaign was conducted between 28th January to 30th January 2017, to test the layout of the advertisement on the Facebook page. Test data was also entered into the online questionnaire at surveymonkey.com. All test data collected were excluded from the valid data, and was subsequently deleted.

Due to the constraint of time and resources for the research, the Facebook campaign was run over a period between 1st February 2017 to 28th February 2017. For the audience type, the Facebook advertisement campaign was set up to target for English-speaking male and female Australian Facebook users in all states, with age of 18 and above. During the campaign period in Facebook, there were 283,090 people viewed, with the targeted audience of Australian Facebook users 18 years old or higher. The campaign attracted 1,404 click links to the survey page in surveymonkey.com, with 188 completed responses captured in the online survey. The samples collected are treated as convenience sampling nature only and has no intention to represent the opinion of all Australian at the time of survey conducted.

The effectiveness of the Facebook advertisement campaign, the conversion rates of the Facebook campaign, were listed with different bases as follows. A rate of 0.0664% of Facebook users who viewed the campaign ad in Facebook and then finished the survey, to a rate of 13.39% of Facebook users who clicked on the campaign ad in Facebook and then finished the survey.

The result of the questionnaire on “Implementation of biometric-based cloud passport in Australia” is discussed below in greater detail. A graphical representation of the distribution of each of the answers is also shown.

5.2 Analysis of collected data from the questionnaire

Question 1 - By choosing "Yes" below indicates that you are 18 years of age or older, and indicates your consent to participate in this survey.

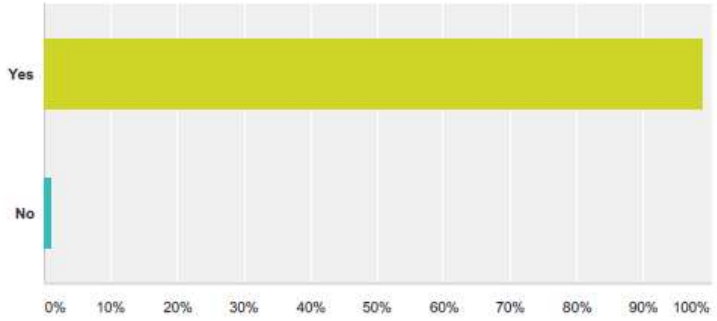


Figure 5.1 – Interviewees over 18 years old and show consent to participate the survey

From figure 5.1, around 98.9% of respondents said "Yes", and there were only two people who said "No". As the survey needs to get consent from interviewees to participate, data from these two people were excluded from the survey data in the subsequent analysis of collected data.

Question 2 - What is your state of residence in Australia?

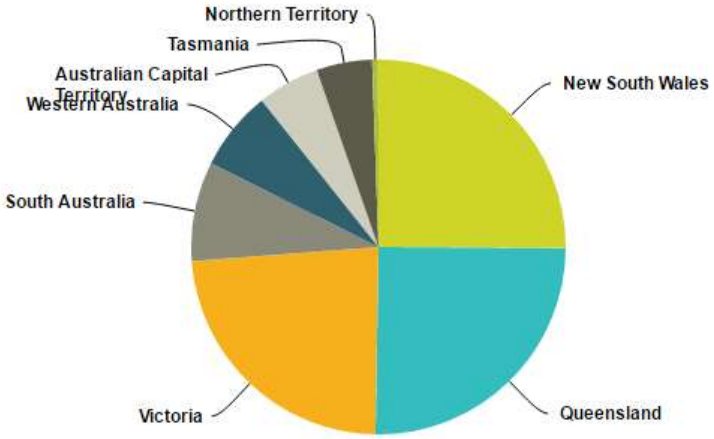


Figure 5.2 – State of residence in Australia

From figure 5.2, most of the participants were in New South Wales (25.1%), Queensland (25.1%), and Victoria (23.5%). Other than the three primary Australian states were South Australia (8.6%), and then a similar portion of participants between the states of Western Australia, Australian Capital Territory and Tasmania. There was only one respondent from Northern Territory.

The result reflected a similar portion of the distribution of the size of the population in the states in Australia (Australian Bureau of Statistics 2016).

Question 3 - What is your gender?

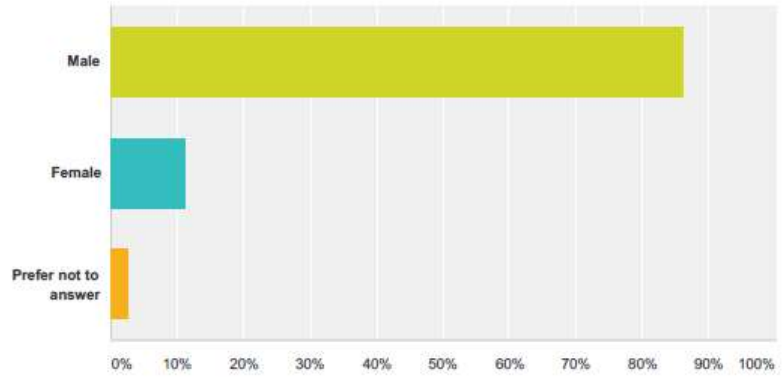


Figure 5.3 – Gender distribution of interviewees

From the responses to the survey as shown in figure 5.3, 86.2% of respondents were male, 11.2% were female, and 2.6% who prefer not to answer the question. The result showed that there was a massive bias to male participants in the survey.

An algorithm in Facebook tries to select the most relevant news feeds and advertisements to each Facebook user's interests (Constine 2016). Based on the algorithm in Facebook, a possible explanation for why there were more male respondents for the survey was because male Facebook users were more interested in technology-related keywords in their Facebook topics, which in turn may show more technology-related survey advertisements to them.

Question 4 - What is your age?

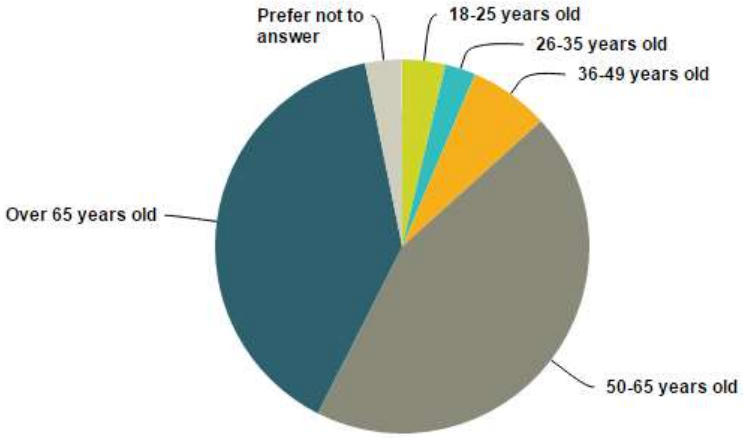


Figure 5.4 – Age distribution of interviewees

From figure 5.4, one found out the majority of respondents were from 50 – 65 years of age (44.2%), and over 65 years of age (39.7%). As the Facebook campaign targeted all Australian users over 18 years old, over 83% of respondents were over 50 years old chose to click on the advertisement and participate in the survey.

The potential bias for respondents over 50 years old was a surprising insight of the survey. As the survey needed approximately 10 - 15 minutes to complete, there may be a possible explanation why young people were deterred from answering all the questions up to the end of the survey. Also, as the portion of people over 50 were probably retirees or semi-retirees, who often stayed at home and accessed Facebook via computers, was probably the reason why they were in the majority portion of all the respondents in the survey.

Question 5 - What is the highest degree of level school you have completed?

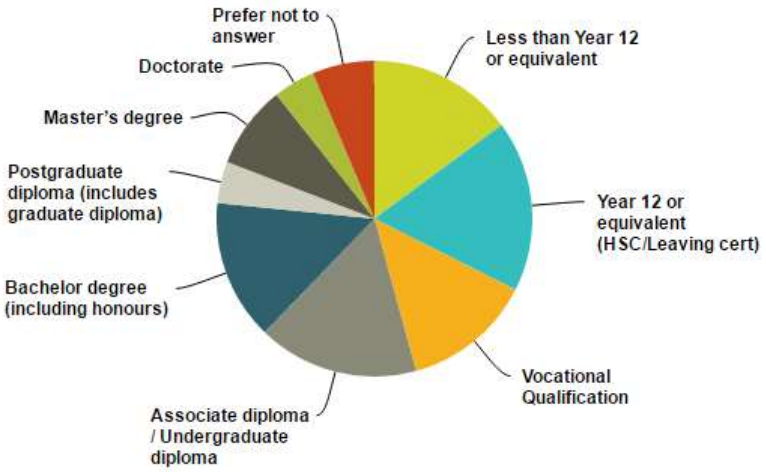


Figure 5.5 – Distribution of education levels of interviewees

From the pie chart in figure 5.5, one can see a majority of respondents were distributed in "Year 12 or equivalent" (17.6%), "Associate and Undergraduate diploma" (16.5%), "Less than Year 12 or Equivalent" (14.9%), "Bachelor Degree (including Honours)" (14.4%) and "Vocational Qualification" (13.3%). Besides that, 4.3% had a Postgraduate or Graduate Diploma, 8.5% had a Master degree, and 4.3% had a Doctorate level of qualification. Around 6.4% of respondents preferred not to answer this question.

Question 6 - Which of the following most closely matches your job title?

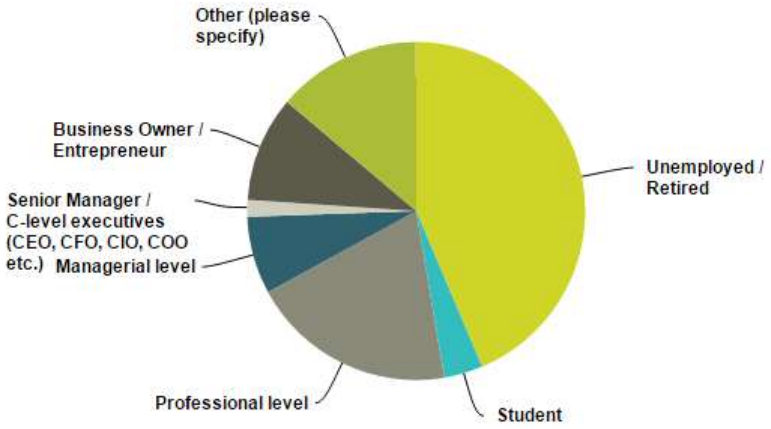


Figure 5.6 – Distribution of employment status of interviewees

From the survey results in figure 5.6, one can see a significant portion of respondents (43.6%) were unemployed or retired. There were 19.7% of respondents who had a professional qualification. There were also 10% of respondents who own a business or are entrepreneurs. As it was shown from Question 4, over 83% of respondents were over 50 years old. Most of the participants were probably retirees, and hence a possible explanation that there was a significant portion of those interviewed (43.6%) were unemployed or retired.

Question 7 - Do you have a passport (travel document)?

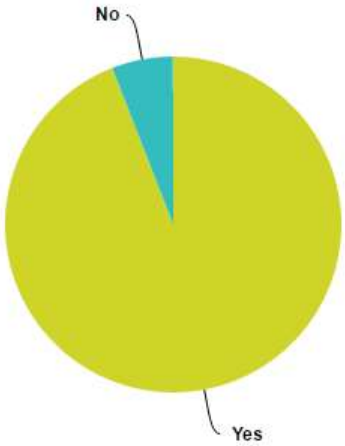


Figure 5.7 – Passport ownership of interviewees

From figure 5.7, there were 94.1% of respondents own a passport, and only 11 out of 186 respondents do not have a passport.

Question 8 - If yes (has a passport), which country or region is your passport issued?

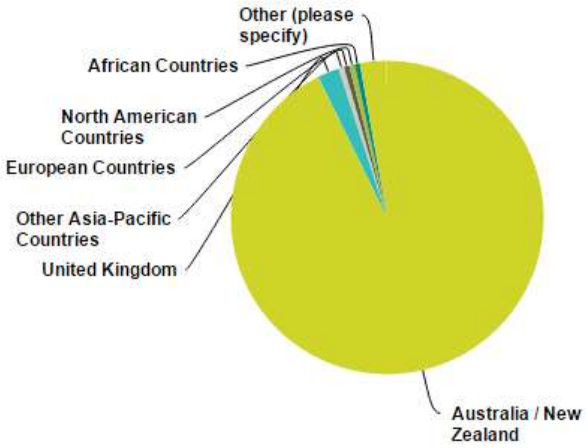


Figure 5.8 – Countries of which passports were issued

From the result in figure 5.8, one found most of the respondents (92.7%) had an Australia or New Zealand passport, with the remaining data scattered across different countries on passport issue. From the data, one can conclude that most of the respondents were either Australians or New Zealanders.

Question 9 - How frequently do you travel overseas per year?

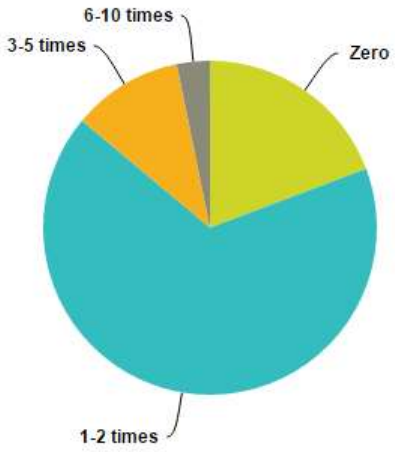


Figure 5.9 – Frequency of travel overseas

From figure 5.9, over one-third of respondents (66.8%) travelled to overseas 1-2 times in a year. 9.3% of respondents did not intend to travel at all, while 10.7% of people travelled more than three times per year.

Question 10 - Which country or region in the world have you travelled before, or intend to travel to in the future (Can choose one or more options)?

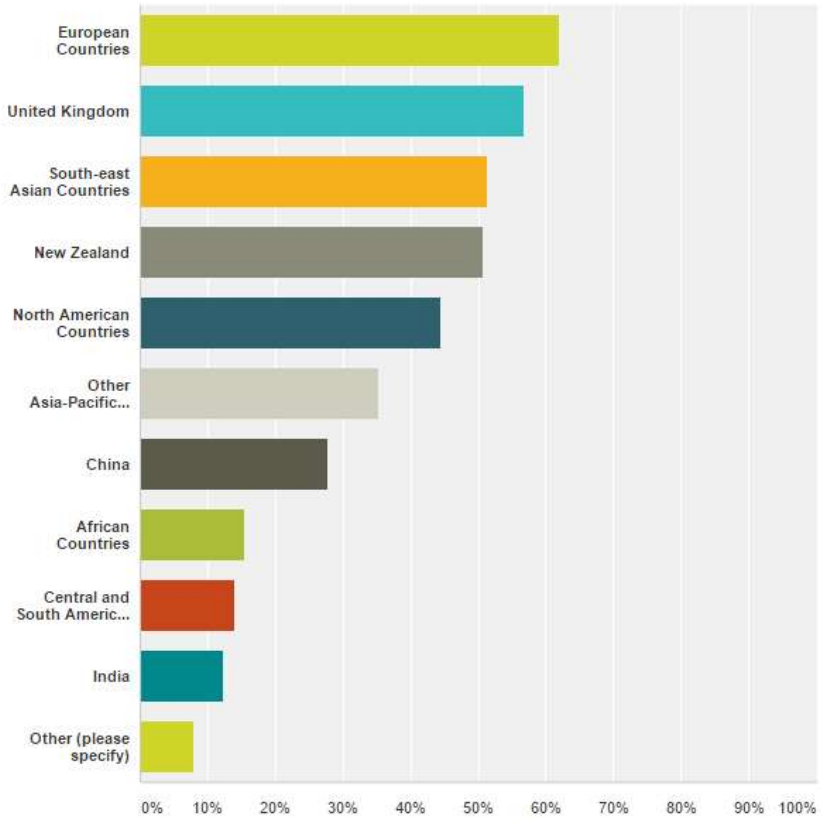


Figure 5.10 – Country or region in the world travelled or intended to travel

Of all the collected data shown in figure 5.10, 62.0% of people intended to go to European countries, 56.7% to the United Kingdom, 51.3% of South-east Asian countries, 50.8% to New Zealand, 44.4% to North American countries, 35.3% to Other Asia-Pacific Countries and 27.8% of people would like to go China. African Countries, Central and South American Countries and India were also among the major countries that were chosen by the respondents.

Question 11 - What is the main reason for travelling overseas?

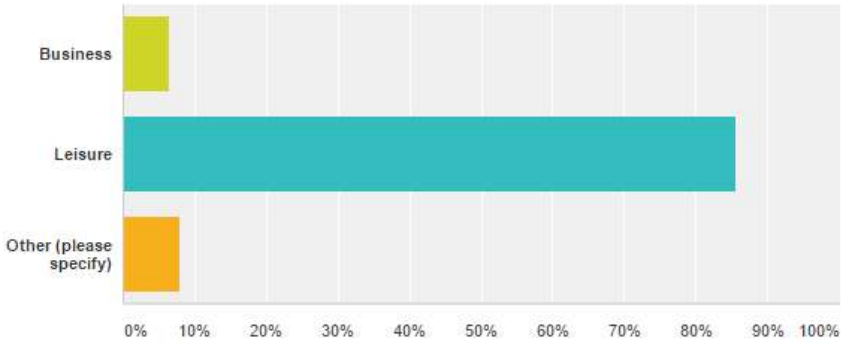


Figure 5.11 – Main reason for travelling overseas

From the result in figure 5.11, there were 85.6% of respondents travelling overseas for leisure. Only 6.4% of responders chose to travel for a business purpose.

Question 12 - Do you favour on the idea of Cloud Passport, which identifies travellers by biometric information (such as facial recognition, fingerprints, iris), without the need of a physical passport (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?

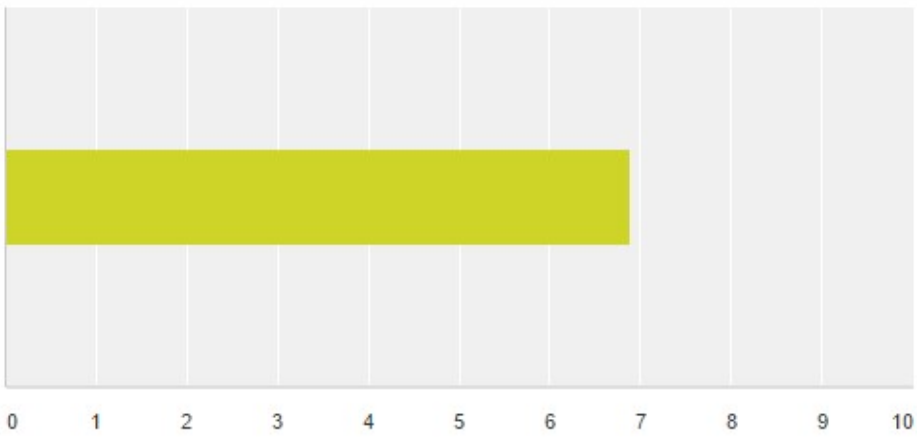


Figure 5.12 – The level of acceptance of the idea of Cloud Passport

There were 183 responses to question 12. Of all the answers collected in the survey, the overall average score for the question was 6.85 (as shown in figure 12). That is, around 68.5% of interviewees agreed with the idea of the Cloud Passport. The observations to carry out bivariate analysis on the result of question 12 with other questions were shown as below.

- When conducting bivariate analysis with question 3, "What is your gender?", by observing figure 13, there were 70.1% of male respondents accept the idea of Cloud Passport, and only 58.6% of female respondents agreed with the idea introduced.

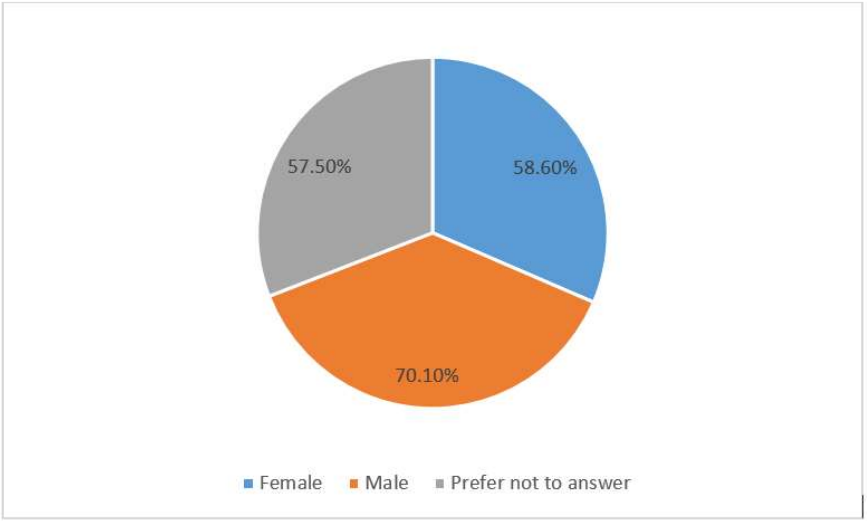


Figure 5.13 – Percentage of acceptance by gender on the idea of Cloud Passport

- When analysed with question 4, "What is your age?", one found from figure 14 that a relatively lower acceptance rate for respondents with age between 18 – 25 (64.3%) and 36 – 49 years old (49.2%). All the other age ranges had an average acceptance rate over 70%. Also, the idea of Cloud Passport had the highest acceptance rate of 87.5% in the interviewees of range 26-35 years old.

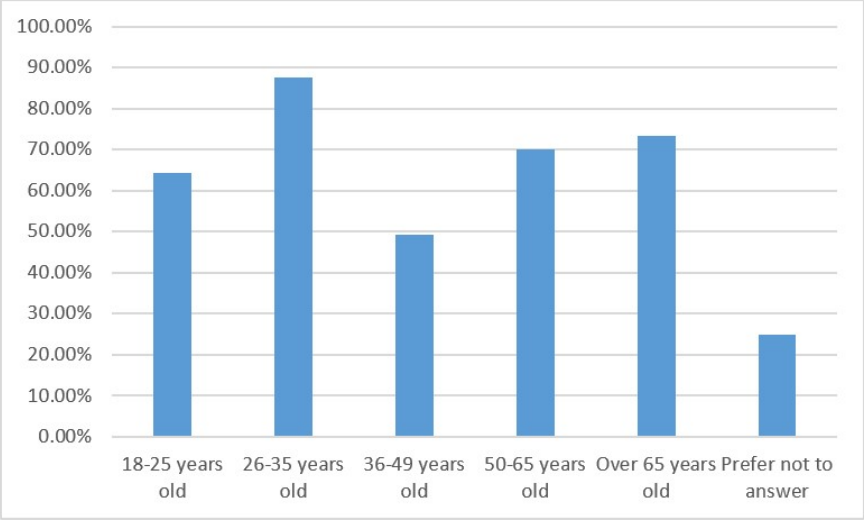


Figure 5.14 – Percentage of acceptance by age on the idea of Cloud Passport

- When analysed with question 5, "What is the highest degree or level of school you have completed?", one can see from figure 15 that the idea of Cloud Passport was more acceptable with respondents with Vocational Qualification (85.6%), followed by Less than Year 12 (77.5%), Postgraduate Diploma (76.3%), Year 12 or HSC level (70.0%) and Associate or Undergraduate diploma (69.7%). Interviewees with Master's degree, Doctorate and Bachelor & honours degree were the ones who were below the overall average of acceptance on the idea of Cloud Passport.

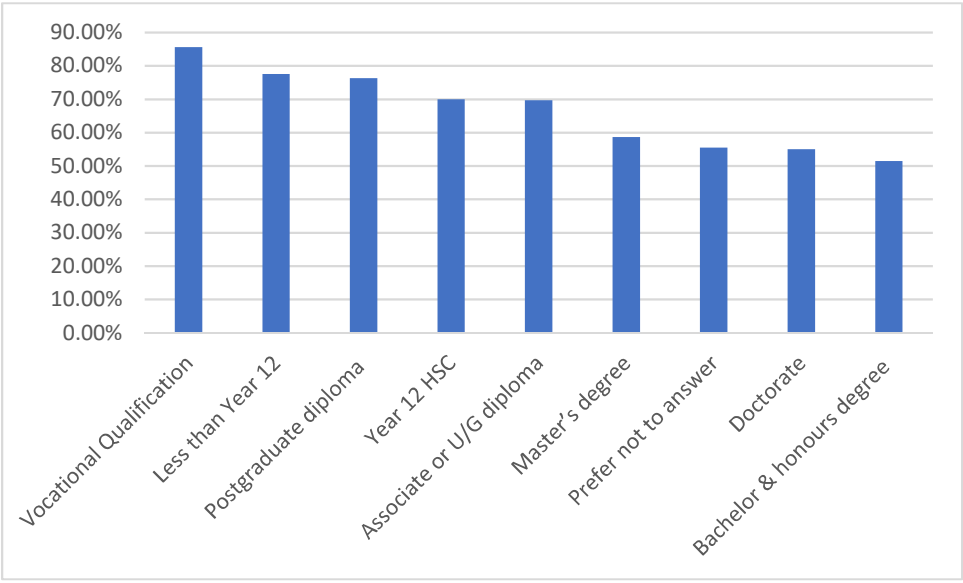


Figure 5.15 – Percentage of acceptance on the idea of Cloud Passport by education level

Question 13 - Do you favour on replacing most of the government personnel with automated border gates when passing through border control in the airport (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?

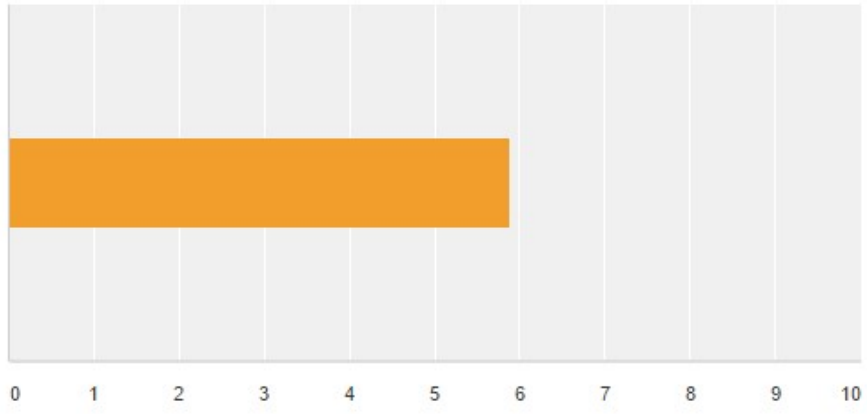


Figure 5.16 – The level of acceptance of the idea of replacing most of the government personnel with automated border gates

From the answers of all the respondents, the overall average score for the question was 5.85 (figure 16). That is, around 58.5% of people favoured on replacing most of the government personnel with automated border gates when passing through border control in the airport. The above result was a surprising outcome from the collected feedback from interviewees, as automated border gates had already implemented in eight major international airports in Australia, to provide a self-help service for border control (Department of Immigration and Border Protection 2017). The details to carry out bivariate analysis on the result of question 13 with other questions were shown below.

- When carrying out the bivariate analysis with question 3, "What is your gender?", one can see from figure 17 that there were 58.4% of male respondents accept the idea of Cloud Passport, and only 55.5% of female respondents agreed with the idea introduced. The four respondents who chose not to reveal their gender type had 75% of acceptance on replacing human with the machine for border processing.

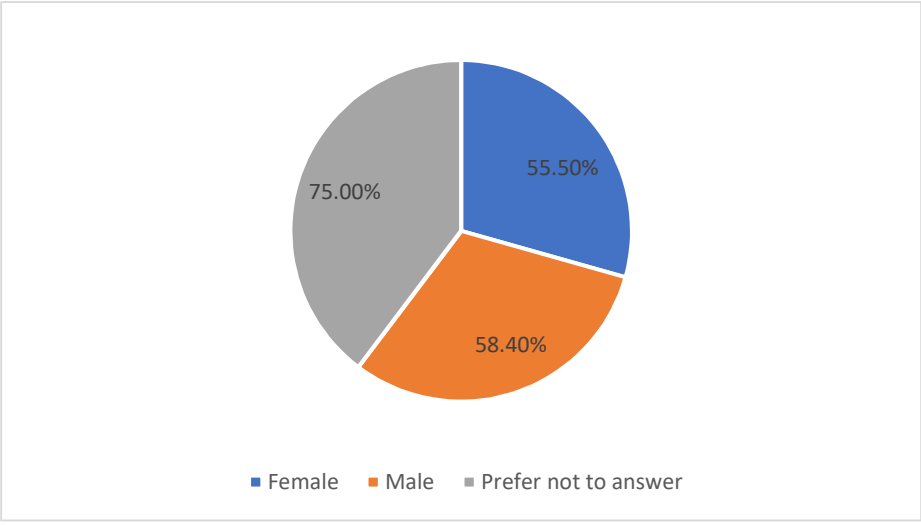


Figure 5.17 – Percentage of acceptance by gender on replacing most of the government personnel with automated border gates

- When analysed with question 4, "What is your age?", one found out from figure 18 a relatively lower acceptance rate for respondents with age between 18 – 25 (32.5%). Respondents in the range of 18 – 25 years old had the highest acceptance rate of the question (72.9%). All the other ranges had similar acceptance rates with the overall average acceptance rate to replace human with the machine for border processing.

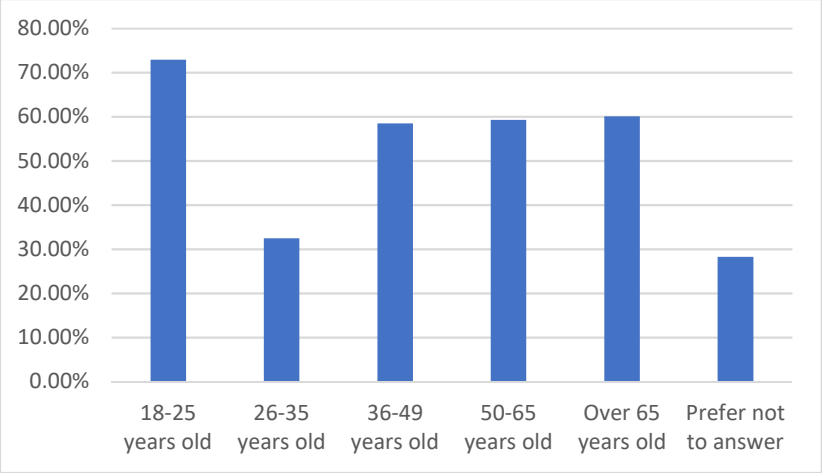


Figure 5.18 – Percentage of acceptance by age on replacing most of the government personnel with automated border gates

- When analysed with question 5, "What is the highest degree or level of school you have completed?", one can see from figure 19 that the idea of Cloud Passport was more acceptable with respondents with Less than Year 12 (68.6%), followed by Associate or Undergraduate diploma (64.8%) and then Vocational Qualification (60.8%). Interviewees with Year 12 or HSC level, Bachelor & honours degree, Postgraduate Diploma, Master's degree and Doctorate and were the ones who were below the overall average of acceptance to replace human with the machine for border processing.

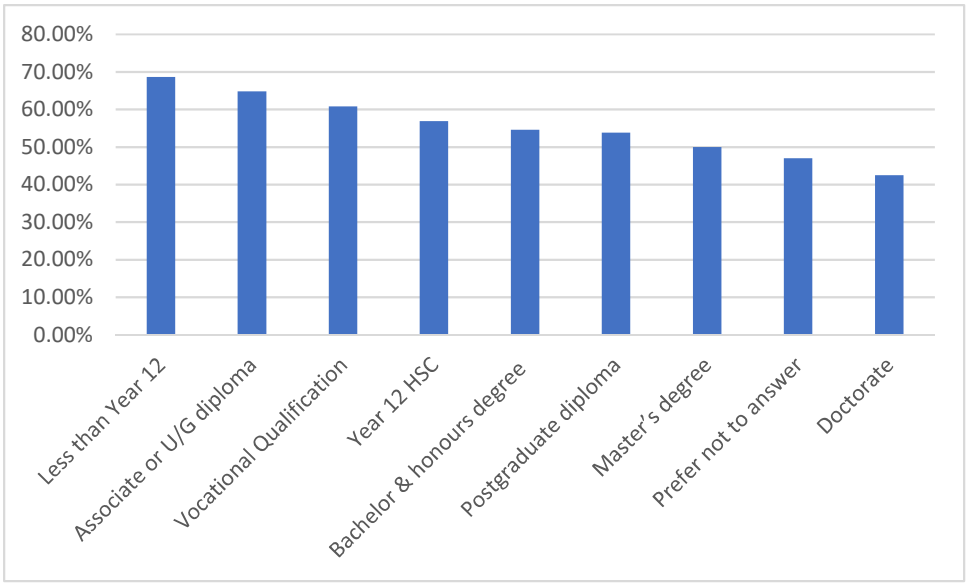


Figure 5.19 – Percentage of acceptance on replacing most of the government personnel with automated border gates by education level

Question 14 - Do you favour on the use of one or more biometric features (face, fingerprint, iris, etc.) to verify the identity of a traveller (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?

Figure 5.20 – The level of acceptance of biometric features to verify the identity of a traveller

The average score of the question of all the responds was 7.57 (figure 20). That is, around 75.7% of people favoured on the use of one or more biometric features to verify the identity of a traveller. The details to carry out bivariate analysis on the result of question 14 with other questions were shown below.

- When carrying out the bivariate analysis with question 3, "What is your gender?", one can see from figure 21 that there were 77.4% of male respondents accept the idea of Cloud Passport, and only 65.2% of female respondents agreed with the idea introduced.

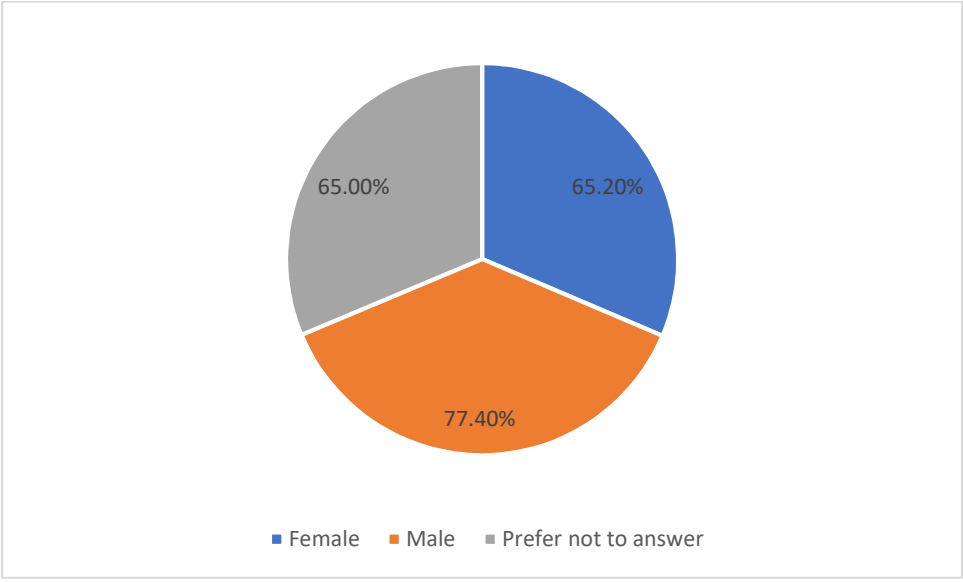


Figure 5.21 – Percentage of acceptance by gender on using biometric features to verify the identity of a traveller

- When analysed with question 4, “What is your age?”, one found out from figure 22 that there was a relatively higher acceptance rate for respondents with age between 26 – 35 (85.0%). All the other age ranges had an average acceptance rate over or equal to 70%.

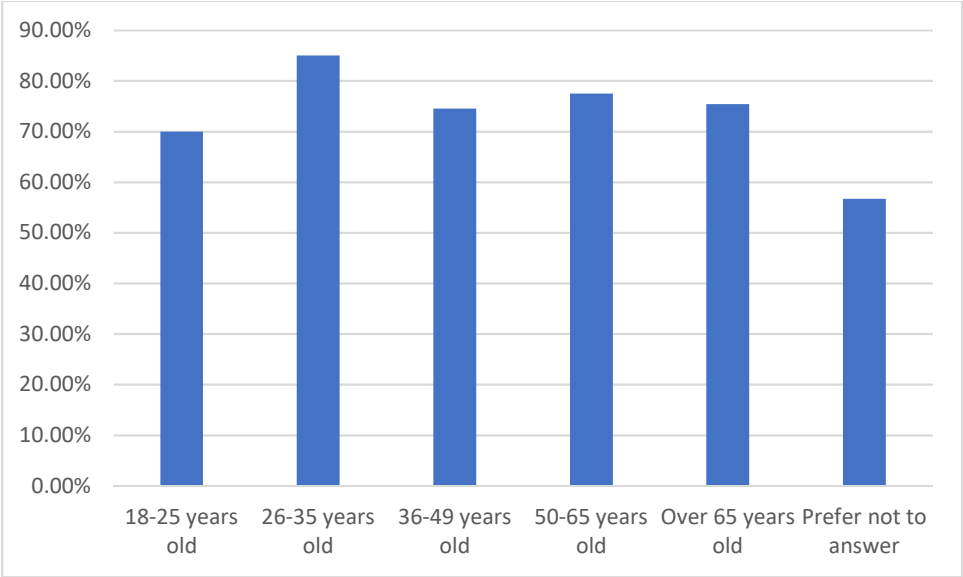


Figure 5.22 – Percentage of acceptance by age on using biometric features to verify the identity of a traveller

- When analysed with question 5, “What is the highest degree or level of school you have completed?”, one can see from figure 23 that the idea of Cloud Passport was more acceptable with respondents with Vocational Qualification (85.8%), followed by Less than Year 12 (79.6%), Year 12 or HSC level (78.8%), and Associate or Undergraduate diploma (76.1%). Interviewees with Postgraduate Diploma, Bachelor & honours degree, Master’s degree and Doctorate were the ones who were below the overall average of acceptance on the idea of Cloud Passport.

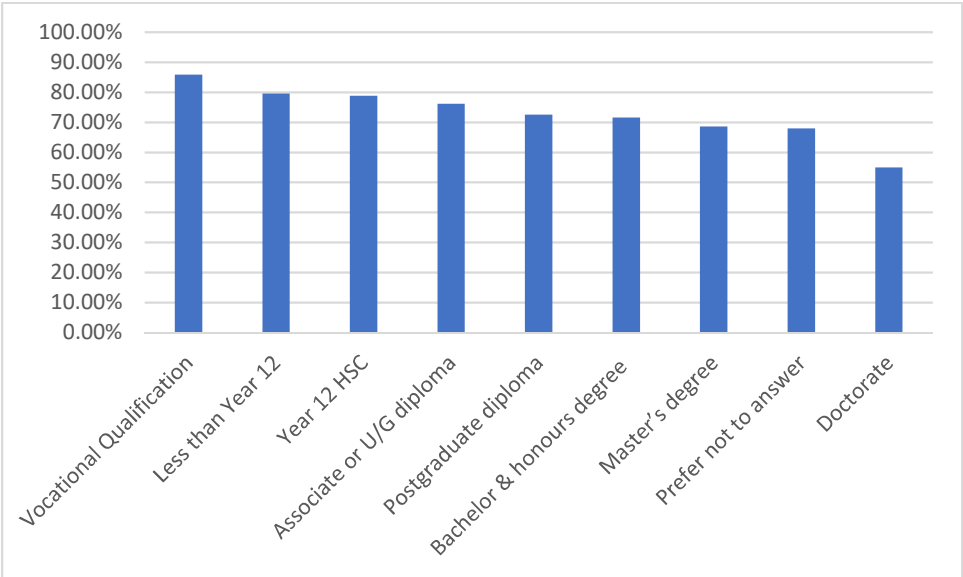


Figure 5.23 – Percentage of acceptance of using biometric features to verify the identity of a traveller by education level

Question 15 - Do you favour on the idea of storing traveller's biometrics features (face, fingerprint, iris, etc.) in a government database, and make available to other countries through a secure cloud-based communication link (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?

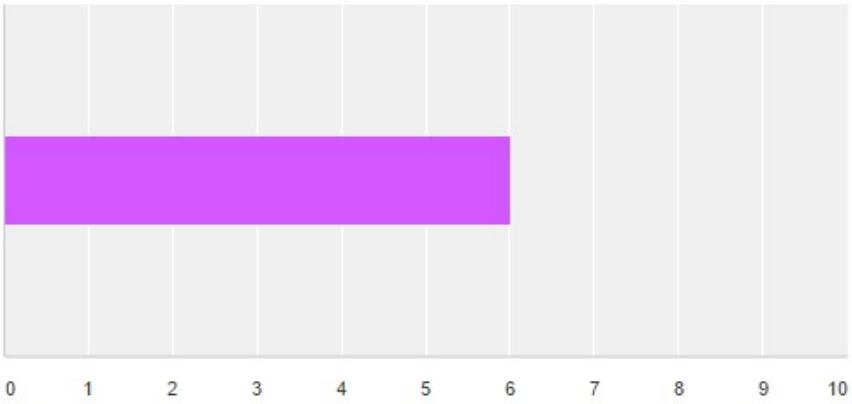


Figure 5.24 – The level of acceptance to store biometric features in a government database, and make available to other countries through a secure cloud-based communication link

The average score of the question of all the responds was 5.98 (figure 24). That is, around 59.8% of people favoured on the idea of storing traveller's biometrics features in a government database and made available to other countries through a secure cloud-based communication link. The observations to carry out bivariate analysis on the result of question 15 with other questions were shown below.

- When carrying out the bivariate analysis with question 3 "What is your gender?", one can see from figure 25 that there were 62.2% of male respondents accept the idea of Cloud Passport, and only 47.1% of female respondents agreed with the idea introduced.

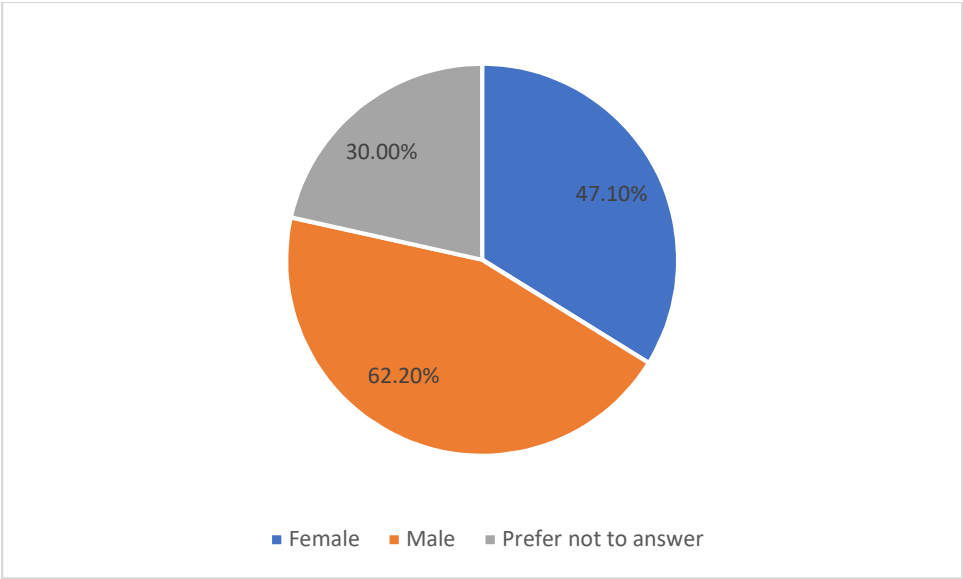


Figure 5.25 – Percentage of acceptance by gender to store biometric features in a government database

- When analysed with question 4, "What is your age?", one found out from figure 26 that there was a relatively higher acceptance rate for respondents with age between 26 – 35 (75.0%). Also, the idea of storing biometric features in a government database had the lowest acceptance rate of 35.4% in the interviewees of range 36-49 years old, while all the other age ranges had an average acceptance rate of 61 - 67%.

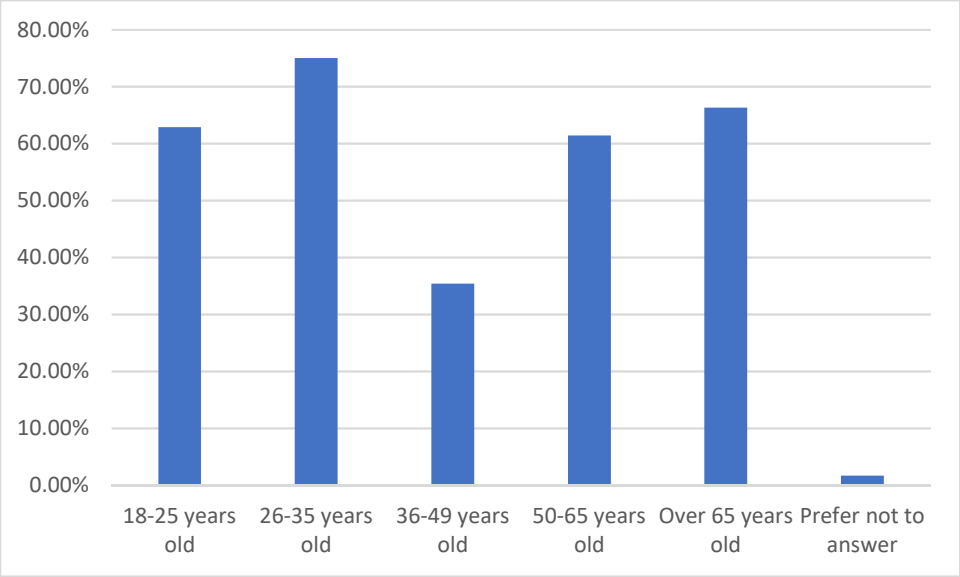


Figure 5.26 – Percentage of acceptance by age to store biometric features in a government database

- When analysed with question 4 "What is the highest degree or level of school you have completed?", one can see from figure 27 that the idea of Cloud Passport was more acceptable with respondents with Less than Year 12 (72.1%), followed by Vocational Qualification (70.0%), Associate or Undergraduate diploma (64.5%), and Postgraduate Diploma (63.8%). Interviewees with Year 12 or HSC level, Doctorate, Master's degree and Bachelor & honours degree were the ones who were below the overall average of acceptance on the idea of Cloud Passport.

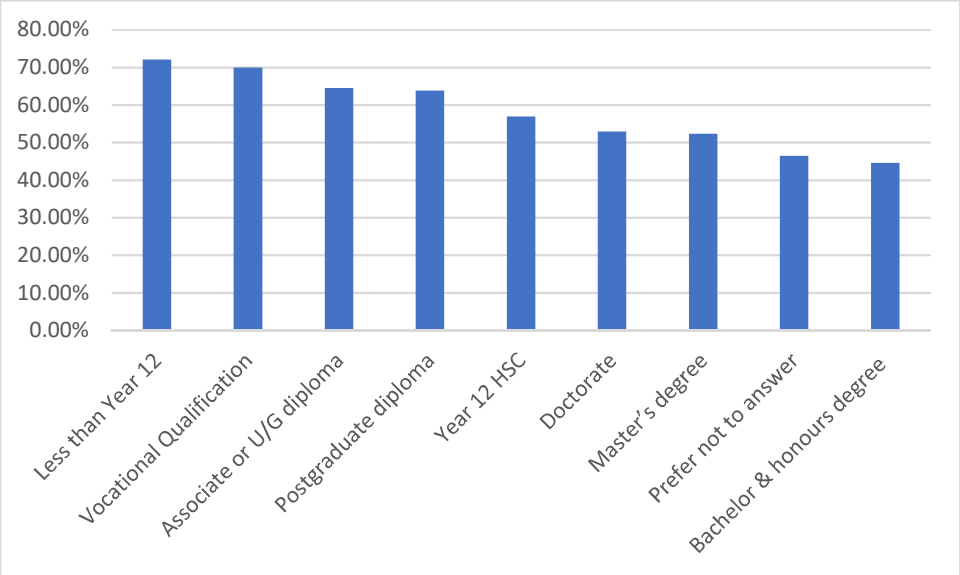


Figure 5.27 – Percentage of acceptance to store biometric features in a government database by education level

Question 16 - Do you think the concept of Cloud Passport will be widely used in countries around the world in the next 10 – 20 years?

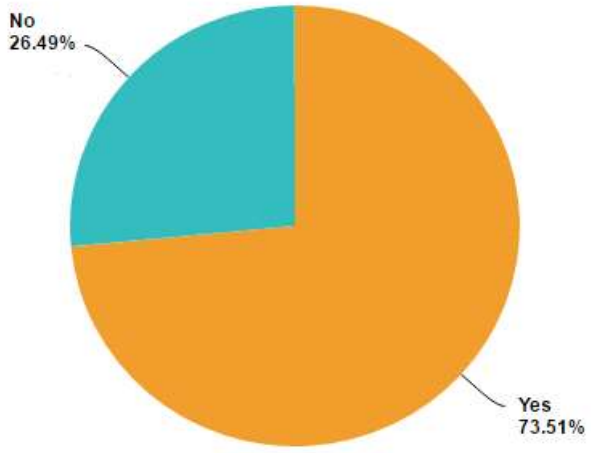


Figure 5.28 – Opinion on whether the concept of Cloud Passport will be widely used in countries around the world in the next 10 – 20 years

Of a total of 184 valid answers, there were 134 "Yes", and 47 "No" (figure 28), and three of the answers were left blank. There were in overall 73.5% of people agreed that the concept of Cloud Passport will be the way of the future and would be widely used in countries around the world in the next 10 – 20 years.

5.3 Summary

A questionnaire on the "Implementation of biometric-based cloud passport in Australia" was conducted in February 2017. Of 185 valid responses to the questionnaire, around 70% of interviewees agreed on the concept of cloud passport. A bivariate analysis was performed on Questions 12 to 15, against questions on gender, age group and educational level.

Observations of the survey results showed that there was a massive bias to male respondents in participating the survey. The potential bias to the respondents over 50 years old was also a surprising insight of the survey. Most of those respondents were probably unemployed or retirees, while younger Facebook users have a lower participation rate when compared with respondents over 50 years old.

On the question of the implementation of the Cloud Passport, an above average acceptance rate was recorded on the acceptance of the concept of Cloud Passport, the extent of use of automated border gates when passing through border control, the use of biometric data for identification, and the idea to store traveller's biometrics data in government databases and make available to other countries.

Opinion on whether the concept of Cloud Passport will be widely used in countries around the world, there was an overall 73.5% of people agreed that the idea of Cloud Passport will be the way of the future and would be widely used in countries around the world in the next 10 – 20 years.

In the next chapter, the qualitative analysed result on the free-form answers for question 17 of the survey is to be discussed.

Chapter 6 – Qualitative Result Analysis

6.1 Introduction

In this chapter, the results of Question 17 in the survey will be elaborated. The main emphasis of this chapter is to perform a textual analysis of the free-form text question on the acceptance of implementation of Cloud Passport and to state the observations from the survey results.

Question 17 of the survey was: "Any other comments on the survey?". There are 68 responses from all interviewees. As the question involved free-form answers from respondents, some efforts were needed to read through the responses in detail and to identify keywords for coding purposes. NVivo, a qualitative software tool, was chosen as the software to carry out the initial text analysis of the free-form texts.

NVivo, by QSR International, is a software for analysing and organising text-based data, and discover insights for qualitative and mixed methods research (NVivo 2017).

As qualitative research produces a significant amount of unformatted textual data either by transcripts or field notes, a Computer Assisted Qualitative Data Analysis Software (CAQDAS) such as NVivo can perform time-consuming and labour intensive data coding and grouping operations, and convert raw qualitative data in a systematic format for further analysis (Zamawe 2015).

NVivo helps the current research to organise data collected from the survey, and then analysed the data with functions provided in the software. From the analysed result by NVivo, insights from unstructured qualitative data in question 17 of the questionnaire can be found.

Based on the qualitative content analysis process introduced by Bengtsson (2016), the analysis of the feedback texts was performed in four stages: Decontextualization, Recontextualization, Categorization and Compilation. The stages of content analysis for results in question 17 of the survey was discussed as follows.

6.2 Decontextualization

An initial analysis of the responses collected from Question 17 is first needed to be broken down into meaningful units (Bengtsson 2016) before any in-depth analysis. The function of "word frequency query" in NVivo was used to extract words that have the high frequency of occurrence. From the list of words from the word frequency query, one can get a feel for what keywords the respondents had expressed on the idea of Cloud Passport.

In the word frequency query function in NVivo, there are options to define the types of a grouping of words, such as "exact matches", "with stemmed words", "with synonyms", "with specifications of the meaning of the words", and "with generalisations based on the meaning of the words". Different word grouping options were chosen for the initial runs of the word frequency query function against the

collected texts from the survey. After some test runs were performed, the choice of grouping types was narrowed down into two options: “with stemmed words” and “with synonyms”. The outputs of both queries were then compared and evaluated on which option should provide the best list of relevant keywords from the raw text data.

Firstly, the word frequency query with the option “With Stemmed words” was run, and the result of the first few most frequently counted keywords, their counts and similar words list were shown in table 6.1.

Word	Length	Count	Weighted Percentage (%)	Similar Words
passports	9	19	2.83	passport, 'passport, passports
security	8	14	2.08	secure, secured, security
countries	9	11	1.64	countries, country
cloud	5	8	1.19	cloud, 'cloud'
biometrics	10	8	1.19	biometric, biometrics
data	4	7	1.04	data
check	5	6	0.89	check, checked, checking, checks
concern	7	6	0.89	concern, concerned, concerns
need	4	6	0.89	need
time	4	6	0.89	time, times

Table 6.1 – Extract of the list of keywords from the result of word frequency query with the option “With Stemmed words.”

From the above list, one can see the words with the same meaning but in different forms were grouped together and added to the count. For example, the word “check” had 6 counts, consists of synonyms of “check”, “checked”, “checking” and “checks”. The keyword list from the current query provided a good starting point to carry out coding of the free-form texts of responses in the survey.

Secondly, word frequency query with the option “With Synonyms” was then run, and the result of the first few most frequently counted words and their similar words were shown in table 6.2:

Word	Length	Count	Weighted Percentage (%)	Similar Words
security	8	26	3.25	certificate, dependent, firmly, good, guarantee, protection, protective, safe, secure, secured, security, strong
passport	8	19	2.83	passport, 'passport, passports
countries	9	12	1.79	countries, country, national
get	3	21	1.7	become, bring, catch, cause, comes, finding, generate, get, let, lets, make, making, started
control	7	16	1.42	check, checked, checking, checks, control, controls, governments, hold, holding, see
data	4	11	1.34	data, information
need	4	11	1.26	asked, need, require, requirements, requires
work	4	16	1.22	acts, bring, forge, form, make, making, process, processing, shaped, turned, work
biometrics	10	8	1.19	biometric, biometrics
cloud	5	8	1.19	cloud, 'cloud'
concern	7	8	1.04	concern, concerned, concerns, worried, worry
time	4	7	1.04	sentence, time, times
trust	5	7	0.97	bank, hope, sure, trust
post	4	7	0.89	cards, carry, office, officer, post, situation
breaks	6	7	0.82	breaks, fail, failed, failing, fails, severe, wear
problem	7	6	0.82	job, problem, problems, trouble
happens	7	6	0.78	finding, happen, happens

Table 6.2 – Extract of the list of keywords from the result of word frequency query with the option “With Synonyms.”

From the above list, one can see more words with related meanings were grouped together compared to the first query. However, some related words associated with the keywords were not the same meaning in context for the current research topic. As an example, the word "security" had 26 occurrences, which consisted of the synonyms "certificate", "dependent", "firmly", "good", "guarantee", "protection", "protective" and "safe", defined in NVivo's vocabulary. Some of the words, when compared with the original texts in the survey, did not have the same meaning as the word "security" from the respondents, which mainly means "border security" or "data security" in this survey. As a result, using the "With Synonyms" option for the word frequency query in NVivo against raw survey free-form texts might produce ambiguous keyword list, which in turn might mislead the meaning of original meaning of the responses in the survey.

In the end, the option of "With Stemmed words" was chosen because NVivo can combine words with the same stem, with different tenses or forms, together in one entry as an outcome. The keyword list from the query result was still in a relatively raw state, and can still be used for further analysis and groupings. A word cloud diagram from NVivo which shows words with the higher frequency of occurrence in a bigger word is shown below (figure 6.1).

Figure 6.1 – Word cloud generated from the result of word frequency query with the option "With Stemmed words."

6.3 Recontextualization

As a list of related keywords was produced from the survey textual data in Decontextualization stage, the entries in the keyword list were inspected to identify words to be included as key content related to the research topic. The criteria used to determine how the words for the research were the words that appeared most frequently in the word list, as well as words that were relevant to the survey topic, such as border protection, cloud technology, authentication and identification.

After evaluation, the first six words from the word frequency query with the option "With Stemmed words" was chosen: they are "security", "passport", "countries", "cloud", "Biometrics" and "data". These

six keywords were then used to perform a text search query in NVivo to find related responses from raw data against the words in the list from the Decontextualization stage. Word tree function in NVivo was used to visualise the relationship between the keywords and phrases from the survey responses. The word tree diagrams of the six keywords were then generated for the illustration of the related phrases in the raw text from the survey.

Firstly, the word tree for the word 'security' is shown in figure 6.2.

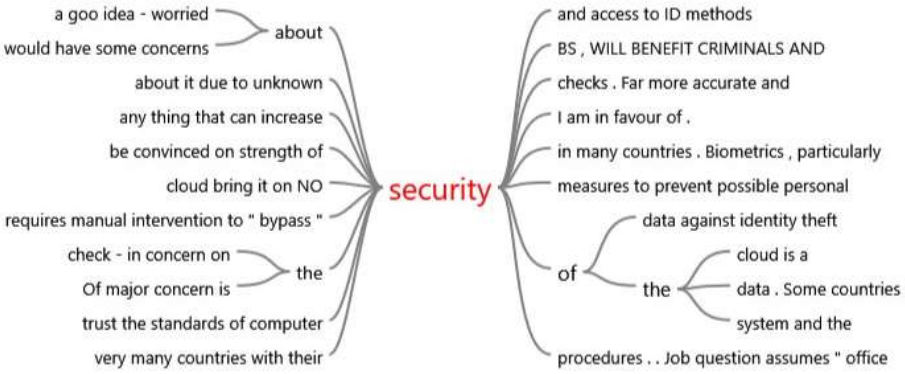


Figure 6.2 – Word tree generated for the word 'security'

From the study of the word tree diagram, the following key contents were found for the keyword 'security': border security, system and data security and privacy.

Next, for the word tree for the word 'passport' (figure 6.3):

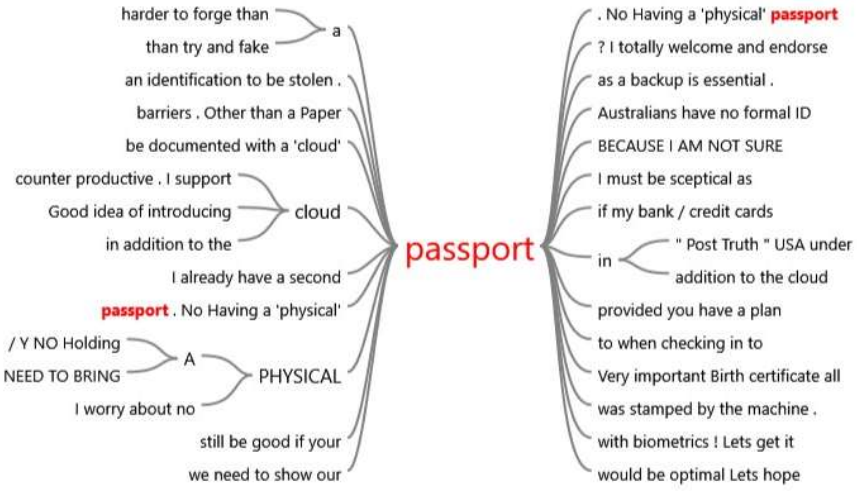


Figure 6.3 – Word tree generated for the word 'passport'

From the word tree diagram the following key contents were found for the keyword ‘passport’: system and data security, identification issues (missing physical passport as ID), multiple passports, fall back procedure when the system failed, not all country has the same technology.

For the word map for the word ‘countries’ (figure 6.4):

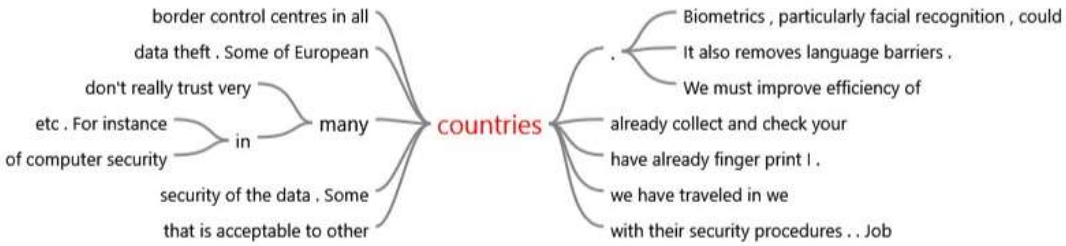


Figure 6.4 – Word tree generated for the word ‘countries’

From the study of the word tree diagram, the following key contents were found for the keyword ‘countries’: border security, data security, improve the efficiency of processing.

On the word map for the word ‘cloud’ (figure 6.5):

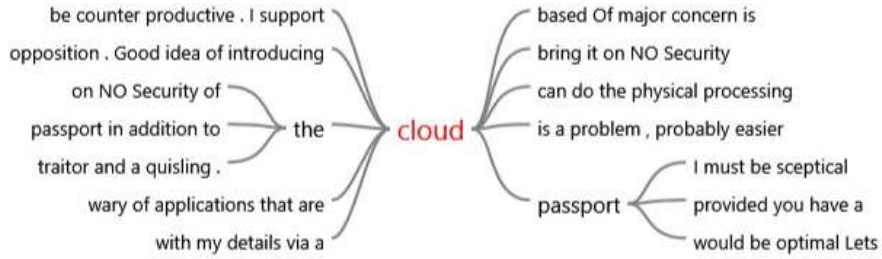


Figure 6.5 – Word tree generated for the word ‘cloud’

The following key contents were found for the keyword ‘cloud’ from the study of the word tree diagram: data security, fall back procedure.

For the word map for the word ‘biometrics’ (figure 6.6):

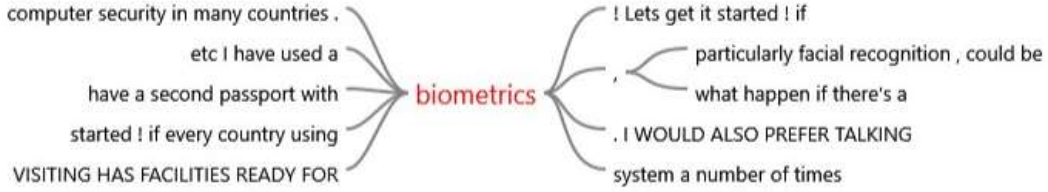


Figure 6.6 – Word tree generated for the word ‘biometrics’

From the word tree diagram, the following key contents were found for the keyword ‘biometrics’: data security, multiple passports, fallback procedure, inconsistencies in the data format and settings in other countries.

Lastly, from the word map for the word ‘data’ (figure 6.7):

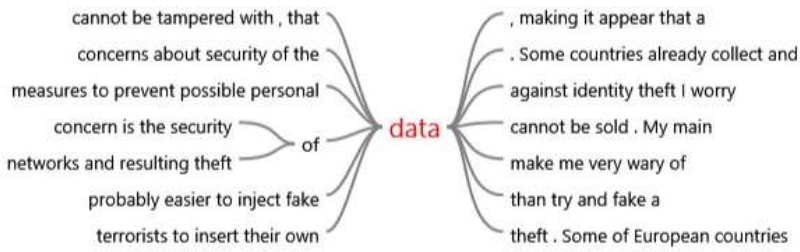


Figure 6.7 – Word tree generated for the word ‘data’

From the study of the word tree diagram, the following key contents were found for the keyword ‘data’: data security, system and data security, concerns about the security in other countries, the threat of terrorists to tamper data.

From the observation above, the observations from the six keywords were combined and formed a list of key topics from the textual survey data as shown in table 6.3 below.

Key Topic	Description
System Security	Secure transmission of data
Data Security	Database not tampered or hacked, stolen data
Technical Issues	How the system is designed; what is the fallback procedure
Identification	How to identify when the physical passport is not available in some cases
Efficiency	Help reduce the processing time
Not Universal	Not all countries have the same technology
Biometrics	Concern on Biometrics
Multiple Identity	How to deal with people with multiple identification documents
Border Control	Tackle terrorism

Table 6.3 – A list of key topics from the textual survey data

Apart from the above outcome, extra efforts were also made to inspect and interpret the raw textual data from the survey manually to extract keywords that can only be deduced from the response texts directly. An example below was shown to illustrate how significant the manual inspection of the survey text. A particular response to Question 17 of the survey was (with inappropriate words masked):

“NO FxxxING WAY....This is just creepy and over the top Big Brother bxxxxxxt.”

While textual analysis software like NVivo could not pick up any relevant keywords from the text, any adult could easily get the underlying meaning the text line was about the concerns of government control when all biometrics data were stored in government. This example showed the importance of carrying out the manual inspection on the response texts from the survey. The following additional key topics were identified with the manual efforts to inspect the raw textual survey data and shown in table 6.4.

Key Topic	Description
Cost Savings	Reduce costs
Government Control	Potential control imposed by government
Change Management	People concerns about changes; reluctant to changes

Table 6.4 – Additional key topics were identified with the manual efforts to inspect the raw textual survey data

6.4 Categorization

With a list of keywords or key topics identified in the Recontextualization stage, the next step was to try to combine keywords with similar meaning among the coded words into groups and bring the core subjects together. The identified key topics could be further grouped into a list of short phrases, which could then be categorised as "Improvements" or "Concerns" on the idea of implementation of Cloud Passport.

The list of groups for the key topics in the "Improvements" category, with examples from the survey results, were:

For Border Control:

> *"Let's stamp out all acts of terrorism , once and for all !"*

For Cost Savings:

> *"Passports are a rip-off, lower the price"*

For Efficiency:

> *"I totally welcome and endorse this idea to obviate lengthy and tiresome queues at immigration and border control centres in all countries. It also removes language barriers."*

The list of groups for the key topics in the "Concerns" category, with examples from the survey result, were:

Change Management:

"The only question I have is what if a female marries/divorces and changes her name, will she be able to change her name as easily as it is now for licences, etc? Without having to go thru the whole application process again."

System and Data Security:

"As much as I see this as the future, I am still not convinced about it due to unknown security measures to prevent possible personal data theft."

"My main concern is hackers. With facial features, those with the knowledge could 'hark' and then build false identities for fraudulent and criminal activities."

Government Control:

"such attempts were made by Hitler, Stalin, etc. etc. and failed. Just another attempt to control everything. There was a sign scratched into a plaster on a pub public toilets in a communist county saying: "Comrades, here only you hold it firmly in hands." Investigation was enormous, endless and severe, but no result. The same comes from "passports". 500 years ago, people had no passports at all and how well they travelled. Border protection must have other priorities."

Technical Issues:

"I support Cloud Passport provided you have a plan b just in case of a computer malfunction."

"If every country using biometrics, what happens if there's a problem of the electronic internet connection."

The above key topic groups with the frequency of the subjects were related to the raw textual survey data could be re-worded into a short phrase as table 6.5.

Key Phrases	Frequency
Better Border Control	1
Concerns about Changes	2
Cost Savings	1
Concerns about System and Data Security	24
Improve Efficiency of Border Crossing	3
Concerns on Government Control	4
Concerns on Technical Issues	21
Subtotal	56

Table 6.5 – key topic groups with the frequency of the subjects were related to the raw textual survey data

A word map diagram of the key phrases to summarise the relationship with their categories is shown in figure 6.8.

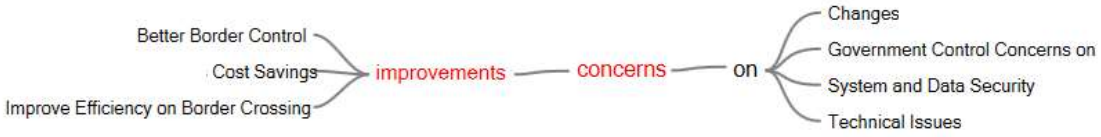


Figure 6.8 – Word map on relations of improvements and concerns

The top two key phrases from the survey texts were also analysed in further details. They are: "Concerns about the system and data security" and "Concerns on technical issues".

The topic of "Concerns on the system and data security" can be summarised into the following areas when referenced to the original textual data from the survey. Firstly, the feedback from the survey concerned whether the level of security was correctly set to disallow unauthorised access to personal data. Secondly, the question of whether there was enough protection to prevent the stored personal data from hacking was raised. There were also doubts about the level of security on the data stored in Cloud-based services. Finally, the question of whether any measures were made to prevent the possible tapping of data transmitted via secured internet transmission link.

On the other hand, the topic of "Concerns on technical issues" can be summarised into the following areas. Firstly, details on how to handle cases when the desired Biometrics information could not be captured (missing eye for iris capture as an example) needed to be addressed. Secondly, it was necessary to have a backup plan available in the situation of system failure. Concerns on how to identify travellers to countries with no Cloud Passport-enabled settings was also raised. Finally, the question of the reliability of internet connection between countries was also raised.

6.5 Compilation and Conclusion

The findings with references the information discovered in the previous stages on the analysis of original texts in the survey were then summarised. There were 68 responses from all interviewees on Question 17 of the survey. The responses were grouped into two categories: the potential improvements from the implementation of the Cloud Passport, and the concerns when implementing Cloud Passport in Australia.

On the category of the potential improvements from the implementation of the Cloud Passport, the survey data showed in "Better Border Control", "Cost Savings" and "Improve Efficiency on Border Crossing.

On the other hand, on the category of the concerns when implementing Cloud Passport in Australia, survey data showed in the area of "Concerns on Changes", "Concerns about System and Data Security", "Concerns on Government Control" and "Concerns on Technical Issues".

Among the key ideas discovered from the survey data, the top two topics from the responses of the survey were “Concerns on the system and data security” and “Concerns on technical issues”. The findings of the two topics were discussed in further details.

The survey results were analysed, and an attempt to draw a summary of insights from the survey data is carried out in the next chapter.

Chapter 7 – Discussion of Survey Results

7.1 Introduction

At the beginning of the chapter, the details of the survey conducted and the metrics of the responses from the survey were revisited. Different parts of the questionnaire and the summary of the data collected was then stated. Some findings and observations from the survey are then discussed in more detail, followed by a formal interpretation of the survey led to a response to the research question. At the end of the chapter, suggestions for the improvement of the survey method are then discussed.

7.2 Summary of the collected data from the survey

A survey was conducted between 1st February 2017 to 28th February 2017 to seek the opinion from Australian public on the implementation of Biometrics-based Cloud Passports. The online questionnaire of the survey was promoted through Facebook social network platform, to reach out all Australian Facebook users who were eighteen years or older.

At the end of the survey period, there were 188 completed responses captured in the online questionnaire. Among the completed questionnaires, 186 of the responses have chosen 'Yes' to give consent to participate the survey. The other two not valid responses were discarded.

The result of the survey was divided into three parts. In the first section of the questionnaire, the demographic information of the interviewees and the travel-related information of the respondents were captured. In the next part of the survey, the interviewees were asked questions about the level of acceptance of the idea of Cloud Passport, the use of automated border gates instead of government personnel, the use of personal biometrics to verify identities, and the idea of storing personal biometrics data centrally or to transmit through a secure cloud-based communication link. A question on whether the concept of Cloud Passport will be widely used in the world in the next 10 – 20 years was also listed. A free-form text box was then provided to allow interviewees to comment on the topic of Cloud Passport.

Both qualitative and quantitative analyses were conducted on the collected data. A summary of the analysed results of the survey is shown below.

7.2.1 Answers on demographics details of the respondents

The first part of the questionnaire, which ranges from question 2 to question 11, revealed that the 186 respondents are distributed across all states of Australia. The percentage of the number of responses by states were in a similar percentage of the population distribution by states in Australia in 2013. The education level of the interviewees was also equally-distributed in the survey results. Over 94% of the respondents have an Australian passport, and 85.6% of them travel overseas mainly for leisure, with a small proportion of 6.4% of respondents travels for business.

Apart from the above, one saw that 86.2% of the interviewees were male, with only 21 females participating in the survey. From the result, one can deduce that male Australian Facebook users might have more interest in technology related posts and surveys. Also, about 85% of respondents were over 50 years of age, with 43.6% unemployed or retirees. This observation indicated that older Facebook users might have more time to complete the whole survey when compared with Facebook users in other younger age ranges.

7.2.2 Answers related to the level of acceptance of Cloud Passport

The second part of the survey, ranging from question 12 to question 16, was set to find out the degree of acceptance of the idea of Cloud Passport, as well as the responses of principal components of the Cloud Passport.

On the result of the feedback of the overall idea of Cloud Passport, an average of 68.5% favoured acceptance of Cloud Passport. In terms of the result by gender, there was on average 70% acceptance level for male interviewees and 58.6% for females. This showed that female interviewees were less in favour of the idea of a Cloud passport. In the age range perspective, there were 87.5% of the level of acceptance on Cloud Passport among interviewees aged 18-25 and 70% of acceptance rate among interview among people over 50 years old. Surprisingly, there are only 49.2% of the level of acceptance on Cloud Passport on interviewees with age range between 36-49. However, as there were only 4 respondents who fell in the age range between 36-49, the result of the acceptance of Cloud Passport for that age range may not represent the actual responses from the age group between 36-49.

On the opinion from the interviewees to replace most of the government personnel with automated border gates when passing through border control at the airport, an average of 58.5% of acceptance level favours the use of automated border gates for border control. This result was much less than the acceptance rate on the overall idea of Cloud Passport, although automated border gates were already introduced in the main airports in Australia. If the result was analysed by gender, there was on average 58.4% acceptance level of using automated border gate among male interviewees and 55.5% of female respondents. In terms of the result by age range, young people in the 18-25 age range were 72.9% in favour of the use of automated border gates, with people over 50 years old were within the average range of acceptance of automated border gates. There was only 32.5% level of acceptance for respondents within the age of 26-35 years old.

When asked about the use of one or more biometrics features (face, fingerprint, iris, etc.) to verify the identity of a traveller, the result survey showed an average of 75.7% of level of acceptance in favour of the use of biometrics technology for identification, which, in surprise, was the highest favorable outcome in the components of Cloud Passport. In terms of the difference in gender, there was a 77.4% level of favourite for male, and a 65.2% for female in the same question in the survey. When the data was analysed across the age range, one can see that biometrics method was well accepted across all age ranges, with an acceptable level of 70.0% for people aged 18-25, and an acceptance rate of over 75% for interviewees over 50 years old. A surprise of 85.0% acceptance rate on respondents with age within 26-

35, which was a sharp rise in the acceptance level when compared to the degree of acceptance of automated border gates.

On the idea of storing traveller's biometrics features (face, fingerprint, iris, etc.) in a government database, and make available to other countries through a secure cloud-based communication link, there is on average a 59.8% of the level of acceptance which favours the idea. The result told us that while the respondents accept the use of biometrics for identification purposes, they did have concerns on how the personal data was stored within government departments, as well as how the secure the biometrics data when used by other countries. A more detailed analysis showed that there was a 62.2% acceptance rate for male and 47.1% acceptance rate for female, which revealed that female interviewees had more concerns about the how the biometrics data is stored and used. In the perspective of age distribution, respondents aged between 18-25 as well as over 50 years are above 60% acceptance rate on the topic. People on age range between 36-49 has the most considerable concern on the security of the biometric data, with only an average of 35.4% of acceptance rate in the survey results.

The last question in the second part of the questionnaire was to seek an opinion on whether the concept of Cloud Passport will be widely used in countries around the world in the next 10 – 20 years. The result, in the form of a 'Yes' or 'No' answer, showed that there was an average 73.5% of total respondents agreed that the concept of Cloud Passport would be widely used in the world in the future. When the result was separated by gender, one can see that there were 75.2% of male respondents who believe Cloud Passport will be widely used in the future and 66.7% for female respondents who agreed. In the perspective of the age range, the result was spread reasonably even across the age range, with the highest 80.0% level of acceptance for interviewees in between 26-35 years old, and the lowest 66.7% level of acceptance in the age range between 36-49 years old.

7.2.3 Free form responses on the Cloud Passport adoption survey

The last question of the questionnaire let the interviewee put in free-form text on feedback on the survey on Cloud Passport. Results from the survey showed 68 interviewees had entered feedback, in which 12 of them are either 'yes', 'no' answers, or a short sentence on agree or disagree on the survey topic. As the 'yes' and 'no' answers were too trivial, they were discarded from further analysis. As a result, a qualitative analysis was then performed against the remaining 56 feedback texts collected. The analysed result was categorised into several key phrases to show the reasons on the favour, as well as the concerns, to the implementation of Cloud passport.

On the points which favour the idea of Cloud Passport, the result showed that the Cloud Passport system could bring in improvements on better border control, with the advantage of cost savings and improved efficiency in handling the increasing flow of travellers at border gates.

On the other hand, the concerns on the implementation of Cloud passport, the result targeted the security of data storage in government, as well as the process of transmitting personal data between countries. Questions with similar meaning were raised in the feedback text like what security measures were taken

place to disallow hackers from accessing personal passport data? How secure was the data stored in either Government premises or in the Cloud-based database services? What measures were taken to prevent unauthorised tapping of the data link between countries?

Another primary concern of the implementation of Cloud Passport from the survey was the possible technical issues in the operating of the Cloud Passport model. Sample questions related to this topic can be: what happened if the desired biometrics information cannot be captured (e.g. an eye was missing for iris data capture)? What is the backup plan in the situation of a system failure on Cloud Passport? How to handle the situation in countries which are not Cloud Passport-enabled? How reliable is the secured internet connection between participated countries?

Other concerns on the idea of Cloud Passport are the possibility for the government to misuse personal biometrics data for possible human control purpose and concerns about the uncertainty of the changes from physical passport to Cloud Passport.

7.3 Responses to the Research Question and the Model for the Adoption of Cloud Passport

In the chapter on Research Philosophy, a research model for the adoption of Cloud Passport in Australia was proposed.

When comparing the research model with the analysed result from the survey, one found out that most of the opinions raised in the survey matched with the predicted drivers and barriers for the implementation of Cloud Passport model before the survey was conducted.

A summary of the analysis results from qualitative free text input data draws a list of drivers and barriers against the implementation of Cloud Passport in Australia. Most of the observations from the survey are covered in the original proposed Cloud Passport Adoption model. A comparison between the findings from the survey against the drives and barriers identified in the original Cloud Passport Adoption model is shown below.

Findings from the Survey	Corresponding Drivers and Barriers in the Adoption Model
Better Border Control	Improved security check at borders
Improve Efficiency of Border Crossing	Cope with Increasing flow of travellers
Cost Savings	Cost Effective and Scalable
Concerns on Changes	<None>
Concerns about System and Data Security	Cloud and Internet Security Risks, Privacy on Personal Data
Concerns on Government Control	Distrust to Government Agencies
Concerns on Technical Issues	Cloud and Internet Security Risks

Table 7.1 - Comparison between the findings from the survey against the drives and barriers in the original Cloud Passport Adoption model

From the above table, there is an additional insight from the survey on the barrier for the implementation of Cloud Passport model, which is concerns from the respondents about the uncertainty of the changes from physical passport to Cloud Passport. The new findings need to be added to the original research model for the completeness of social opinion on the adoption of Cloud Passport model.

An improved model for the adoption of Cloud Passport is shown in figure 7.1 (the new finding for the research model is shown in blue).

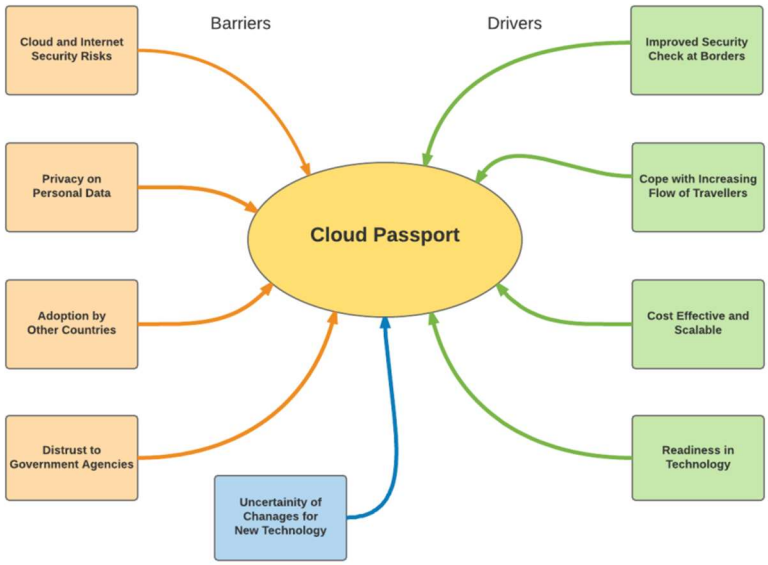


Figure 7.1 - A Revised Cloud Passport Adoption Model

The revised Cloud Passport adoption model gives a clearer picture of the social opinion from Australian people on this topic, which may help to create a plan for the implementation of Cloud Passport.

7.4 Limitations of the survey

Below are the observations on the improvements to the survey on Cloud Passport, with using Facebook as the social media for the promotion of the survey link.

7.4.1 Resources

Firstly, 188 responses for the survey was collected from 1st February to 28th February 2017. In a statistical perspective, for a population size of around 24 million people in Australia (Australian Bureau of Statistics 2017), a sample size of 385 is needed for a more representative level of a survey, with a confidence level of 95%, and a margin of error of plus and minus 5 % (Smith 2013). The reason why there were not enough responses to the current survey was due to limited resources, as it needed more time and money to run a more extended Facebook advertising campaign to achieve the desired number

of responses. As an indication, to achieve more than 385 responses in the current survey, one need to run a Facebook advertisement campaign of an extra half month, plus the extra costs for a more extended Facebook advertisement campaign.

7.4.2 Apparent bias survey result due to Facebook advertisement algorithm

Secondly, Facebook was used to promote the survey link for Australia adult Facebook users. The reason to choose Facebook for the promotion of the survey is that Facebook has 16 million registered Australian users, the highest number of registered Australian users among all social media tools as at January 2017 (Cowling 2017). Facebook can give us a good representation of Australian opinion by promoting the survey link on the Facebook platform. However, weakness of this approach is that Australians with no Facebook accounts will be excluded from the survey. As a result, the participants in the survey did not cover all Australian, especially Australian who are not familiar with the Facebook application.

Another characteristic of using Facebook for advertisement is that the frequency of the advertisements posted on a user's Facebook pages is determined by the interests of individual users. That is a possible explanation that 86.2% of the respondents of the survey were male, as male Facebook users might show more interest in technology-related posts and surveys. In order to get the more female Facebook user to respond to a survey, one could run a separate advertisement campaign to target female adult Australian only and run the campaign for a more extended period in order to collect more survey responses from female Facebook users.

There is a surprising finding that senior people are more eager to participate in the current survey. In our survey on Cloud Passport, about 85% of respondents were over 50 years of age, and 43.6% of interviewees were either unemployed or retirees. A possible reason of this insight is that, while the questionnaire takes about ten to fifteen minutes to complete, people who stay at home may have more time to sit in front of a computer to complete the survey. A shorter version of the questionnaire, with the length of the survey no more than 5 minutes to complete, may attract more young people to participate in the survey. The questions also need to be modified with simple choices only, in order to let participants choose answers quickly. Advertisements on Facebook should also advertise on the smartphone Facebook App in addition to the desktop version of Facebook to attract more Facebook users to respond to the survey.

7.5 Summary

In this chapter, the result of the survey on the idea of Cloud Passport was discussed by using results from the quantitative analysis in the first 16 question of the survey, and qualitative analysis of Question 17. Overall, the acceptance level on the implementation of Cloud Passport is 68.5%, with an average of 73.5% of total respondents agreed that the concept of Cloud Passport would be widely used in the next 10 to 20 years' time. A breakdown of the responses by gender and by age group for each key question was also presented. The chapter ends with some discussion on the use of Facebook as an advertising

medium to the survey, and some lessons learnt to use Facebook more efficiently for future references when conducting surveys online.

Chapter 8 – Conclusion

8.1 Summary of the Research Result

In the chapter on Research Philosophy the research questions were stated as follows:

> *RQ 1: Given the current level of technology that enables a Cloud Passport model - what are the opinions of select members of the Australian general public to the adoption of a cloud passport?*
>
> > *RQ 1a: What are the concerns of a sample of Australian with regard to replacing the current physical passport with a digital version?*

In order to respond to the research questions, one needs to seek an opinion from the Australian general with a view to having a smooth implementation of the Cloud Passport system. A survey was conducted in February 2017 to find out the social attitude on the level of acceptance on the proposal of Cloud Passport by the general public in Australia. The survey, which was promoted by advertisement on Facebook social media, consists of three different parts. The first part is to understand the composition of the Australian general public whom giving an opinion on the research subject. The second part is to question the quantitative nature regarding the level of support of the cloud passport idea, and on different components that constitute the implementation of cloud passport. The third part is to give the interviewees a text box, to enter their general feedback about the proposal of cloud passport.

The collected data were then analysed both quantitatively and qualitatively, to determine reactions and trends of public opinion on Cloud Passport.

The survey collected responses from 186 adult Facebook users throughout Australia. The survey results showed that the average acceptance level on the idea of cloud password is around 70%. While there is a high level of the use of one or more biometrics features (face, fingerprint, iris, etc.) to verify the identity of a traveller, the interviewees rated low in both replacing most of the government personnel with automated border gates, as well as storing traveller's biometrics features in a government database, and potentially sending personal data to other countries for authentication and identification purposes.

75% of the interviewees thought that cloud passport would be available throughout the world in the next 10 to 20 years. More detailed analysis of the survey data is also presented in the previous chapters of the thesis.

A textual analysis of the feedback from the survey also showed that the Cloud Passport system could bring improvements on better border control, with the advantage of cost savings and improved efficiency in handling the increasing flow of travellers at border gates.

On the other hand, the survey showed concerns about the security of data storage as well as security threats in the process to transmit personal data between countries. They also expressed concerns about the possible technical issues in the operating of the Cloud Passport model. The possibility for the government to misuse personal biometrics data for possible human control purpose and concerns about the uncertainty of the changes from physical passport to Cloud Passport were also expressed in the analysis result of the survey.

The observations from the surveys formed an overall result in the opinion of Australians on the Cloud Passport initiative. The collected opinions can help to build an appropriate change management strategy and to enable a successful rollout of cloud passport in Australia.

8.2 Limitation of the Research

The boundary conditions of the current research on the social attitude of Australian on the topic of Cloud Passport are list below. Firstly, the survey did not cover all Australians as the scope of the interviewees for the survey were limited to Facebook users only. Australians with no Facebook accounts were excluded from the study.

Secondly, the result of the survey showed that about 85% of respondents to the survey were over 50 years of age. Most of the interviewees were male Facebook users. The result of the survey did not reflect the opinions of female Facebook users.

Finally, the survey captured views from Australian people only. Opinions on the implementation of Cloud Passport from other countries were not within the scope of the current research.

8.3 Opportunities for Future Research Area

As the research has captured some findings on the social responses to the idea of Cloud Passport, there is also room for further studies, so that there will be a continuous improvement for the implementation of the passport-less border crossing system, which can then be accepted by the people in Australia.

The first area for possible future research is to extend the domain of the survey to Australians who may not have a Facebook account. It may be in the form of a paper version of the questionnaire, with a convenient sampling to obtain opinions from people in the main cities of Australia. In this way, one can capture their view of the idea of Cloud Passport from a different group of the Australian public, and help to figure out a better change management procedure for the implementation of Cloud Passport.

Secondly, the same survey can be repeated at various stages of the implementation of Cloud Passport system. The results of the surveys conducted at different times can then be compared to understand the evolution of the feedback on the stages of implementation and the effectiveness of the change management procedures.

Another suggestion for future research is to have a separate survey to target younger Australians on their views of Cloud Passport. As a majority of the respondents in the survey are over 50 years old, a similar survey of younger Australians can capture more opinion on Cloud Passport in different age groups. The potential result from the suggested survey can combine with the current survey results, and give a better representation of the social responses to the idea of Cloud Passport.

Finally, a similar survey on the acceptance of Cloud Passport can be conducted in other countries which have the capacity to implement passport-less border crossing system. The data collected can help to understand the social attitude on the idea of Cloud Passport from other countries, and hence contribute to engaging other countries to join in the Cloud Passport model.

The above suggestions of future research areas can help the Australian government to implement a more efficient passport-less border crossing system, in order to have a seamless experience for travellers, as well as to enable a thorough identification and authentication of passengers at border gates, for more robust prevention from potential terrorist threats.

This Page Intentionally Left Blank

References

"Airport Traffic Data - January 2017", (2017). Bureau of Infrastructure, Transport and Regional Economics. Viewed 23 April 2017, <https://bitre.gov.au/publications/ongoing/airport_traffic_data.aspx>.

"Arrivals SmartGate". Department of Immigration and Border Protection, viewed 26 Nov 2016, <http://www.border.gov.au/Trav/Ente/Goin/Arrival/Smartgateor-ePassportx>.

"Australian Code for the Responsible Conduct of Research", (2007). National Health and Medical Research Council & Australian Research Council, <https://www.nhmrc.gov.au/_files_nhmrc/file/publications/r39_australian_code_responsible_conduct_research_150811.pdf>.

"Australian Government Cloud Computing Policy", Version 3.0 Oct 2014, viewed 30 Apr 2016, <https://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf>.

"AWS Billing and Cost Management - User Guide", Version 2.0 (2016) Amazon Web Service, viewed 30 Sep 2016, <http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>.

"IATA Forecasts Passenger Demand to Double Over 20 Years", (2016). IATA Web Site.

"List of busiest airports by passenger traffic", (2017). Wikipedia: The Free Encyclopedia, Wikimedia Foundation Inc., viewed 23 April 2017, <https://en.wikipedia.org/wiki/List_of_busiest_airports_by_passenger_traffic>.

"What Is a Likert Scale and How to Use It ", Surveymonkey web site, viewed 30 Apr 2017, <https://www.surveymonkey.com/mp/likert-scale/>.

"What is Nvivo?", QSR International web site, viewed on 31 May 2017, <http://www.qsrinternational.com/what-is-nvivo>.

"Working with the AWS Management Console AWS - Management Console", Amazon Web Service, viewed 30 Sep 2016, <http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/gettingstarted.html>.

“Protecting our borders”, (2017). Australian Border Force in Department of Immigration and Border Protection, Australian Government. Viewed 23 April 2017, <https://www.border.gov.au/australian-border-force-abf/protecting>.

"Sydney Airport Traffic Performance December 2016", (2016). Sydney Airport Limited ASX released on 20 Jan 2017. Viewed 23 April 2017, <http://www.sydneyairport.com.au/investors/~/media/files/investors/news%20and%20events/syd%20asx%20releases/2017/170120%20december%202016%20traffic%20release%20circulated%20for%20signoff.pdf>.

Albahdal, A. (2015). Toward secure, trusted, and privacy-enhanced biometrics in the cloud (Doctoral dissertation, University of Colorado at Colorado Springs).

Anderson, T (2013). Research Paradigms: Ontology's, Epistemologies & Methods, Universitat Oberta de Catalunya, Powerpoint presentation, Viewed 30/4/17.

Australian Demographic Statistics, (2016). Australian Bureau of Statistics. Viewed at 15/4/2017, <http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0>

Australian Passports Determination 2005, EXPLANATORY STATEMENT AUSTRALIAN PASSPORTS ACT 2005, viewed 30 Apr 2016, <https://www.legislation.gov.au/Details/F2005L02625/e36f4239-5a0f-465c-91bd-e371fde0492f>.

Avison, D.E. and Fitzgerald, G., (1995). Information systems development: methodologies, tools and techniques.

Baun, C., Kunze, M., Nimis, J., & Tai, S. (2011). Cloud Computing: Web-based dynamic IT services. Springer Science & Business Media.

Baxendale, R. (2017). Shorten fears welfare card is 'harsh treatment just to get a headline. The Australian, 1 Sep 2017.

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L., (2004). International differences in information privacy concerns: A global survey of consumers. The Information Society, 20(5), pp.313-324.

Bengtsson, M., (2016). How to plan and perform a qualitative study using content analysis. NursingPlus Open, 2, pp.8-14.

Bhattacherjee, Anol, (2012). "Social Science Research: Principles, Methods, and Practices". Textbooks Collection. Book 3. http://scholarcommons.usf.edu/oa_textbooks/3.

Bourke, L. (2015). "Australia to trial cloud passports in World-First Move", SMH 29 Oct 2015.

Burrell, G. and Morgan, G., (1979). Sociological paradigms and organisational analysis (Vol. 248). london: Heinemann.

Busch, P., Smith, S., Gill, A., Harris, P., Fakieh, B., & Blount, Y. (2014). A Study of Government Cloud Adoption: The Australian Context. ACIS.

Carter, M. (2013). Secure Identity in Cloud Computing, The Aerospace Corporation, PowerPoint presentation, viewed 30 Apr 2016, <gsaw.org/wp-content/uploads/2013/06/2013s11b_carter.pdf>

Cherdantseva, Y. and Hilton, J., 2013, September. A reference model of information assurance & security. In Availability, reliability and security (ares), 2013 eighth international conference on (pp. 546-555). IEEE.

Children's passports - Australian Passports Act 2005, Australian Passport Office, viewed 31 Aug 2016, <https://www.passports.gov.au/passportsexplained/childpassports/Pages/default.aspx>.

Chou, D. (2011) Internet Service Bus and Windows Azure AppFabric, Microsoft Developer Blog, viewed 30/10/2016, <https://blogs.msdn.microsoft.com/dachou/2011/03/24/internet-service-bus-and-windows-azure-appfabric/>.

Clark, S. R. (2011). Balancing Privacy and Security in the Australian Passport System. Deakin Law Review, Forthcoming.

Constine, J. (2016). "How Facebook News Feed Works". TechCrunch Website, 6/9/2016, Viewed at 15/4/2017, <https://techcrunch.com/2016/09/06/ultimate-guide-to-the-news-feed/>.

Cowling, D. (2017). Social Media Statistics Australia – January 2017, Social Media News web site, viewed 19 Aug 2017, <https://www.socialmedianews.com.au/social-media-statistics-australia-january-2017/>.

Creswell, J.W., (2013). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Creswell, J.W., Plano Clark, V.L., Gutmann, M.L. and Hanson, W.E., 2003. Advanced mixed methods research designs. Handbook of mixed methods in social and behavioral research, 209, p.240.

Duckett, C. (2016). ABS blames Census 2016 site failure on DDoS attack, viewed 15 Oct 2016, <http://www.zdnet.com/article/census-2016-site-falls-to-ddos-attack/>.

Ewing, I. (2015). "New SmartGate aims to decrease airport queues", NZ NewsHub.

Ferbrache, D. (2016). Passwords are broken–the future shape of biometrics. Biometric Technology Today, 2016(3), 5-7.

Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M. and Inácio, P.R., (2014). Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), pp.113-170.

Ford, M., (2015). The rise of the robots: Technology and the threat of mass unemployment. Oneworld Publications.

Galliers, R.D., (1990). Choosing appropriate information systems research approaches: a revised taxonomy. In In Proceedings of the IFIP TC8 WG8. 2.

Goode, A. (2014). Bring your own finger–how mobile is bringing biometrics to consumers. Biometric Technology Today, 2014(5), pp.5-9.

Greenleaf, G., (1987). The Australia Card: towards a national surveillance system.

Greenleaf, G., (1988). Lessons from the Australia Card -- deux ex machina?

Guba, E.G. and Lincoln, Y.S., (1994). Competing paradigms in qualitative research. Handbook of qualitative research, 2(163-194), p.105.

Harrison, (2017). "How Facebook and Survey Monkey can be used for research", Deakin University, Viewed at 14/4/2017, <https://www.deakin.edu.au/__data/assets/pdf_file/0008/709892/Harrison-Facebook-and-Survey-Monkey-and-research.pdf>.

Hartmann & Körting (2009) “The ICAO PKD - Ten good reasons to join”, Keesing Journal of Documents & Identity, issue 30, 2009, p.3-6.

Hirschheim, R., (1985). Information systems epistemology: An historical perspective. Research methods in information systems, pp.13-35.

Hon, W., Millard, C. (2013) Control, Security, and Risk in the Cloud. Cloud Computing Law, Oxford Scholarship Online: January 2014.

ICAO Traveller Identification Programme (TRIP) 2015, PowerPoint presentation, viewed 30 Apr 2016, ICAO Regional FAL Seminar Bangkok, Thailand, 24 March 2015, <http://www.icao.int/ROAF/Documents/meetings/2014/FAL-FEB/Day%203%20-%20ICAO%20TRIP.pdf>.

Jain, Anil, Patrick Flynn, and Arun A. Ross, eds. Handbook of biometrics. Springer Science & Business Media, 2007.

Jamil, D., & Zaki, H. (2011). Cloud computing security. International Journal of Engineering Science and Technology, 3(4).

Jones, R., (2011). Border security, 9/11 and the enclosure of civilisation. The Geographical Journal, 177(3), pp.213-217.

Jordan, R. (2006). Identity cards and the Access Card, Parlimant of Austrlaia, February 2006.

Kalakou, S., Psaraki-Kalouptsidi, V., & Moura, F. (2015). Future airport terminals: New technologies promise capacity gains. Journal of Air Transport Management, 42, 203-212.

Khorshed, M.T., Ali, A.S. and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6), pp.833-851.

Kuhn, T., (1962). The Structure of Scientific Revolutions, University of Chicago Press 1962.

Lee, A.S., (1991). Integrating positivist and interpretive approaches to organizational research. Organization science, 2(4), pp.342-365.

Levin, W.C., (1994). Sociological ideas: Concepts and applications. Wadsworth Publishing.

Locke, C. (2016). "Get creative or else: the pressure's on banks to embrace biometrics". Biometric Technology Today, 2016(6), pp.8-10.

Lodico, M.G., Spaulding, D.T. and Voegtle, K.H., (2010). Methods in educational research: From theory to practice (Vol. 28). John Wiley & Sons.

Lokhande, T. S., & Shelke, R. R. (2013). A Review Paper on Cloud Computing Security. International Journal of Advanced Research in Computer Science, 4(6).

Lynch and Bennett (2015) “Beyond the book - A model for virtual passports”, Keesing Journal of Documents & Identity, Annual Report Identity Management 2015-2016, p.3-6.

Lynch, M. (2016). "Your Face Your Passport : Prospects for a biometric passport", PowerPoint presentation, viewed 26 Apr 2016, Biometrics Institute Asia-Pacific Conference 2016, <http://www.biometricsinstitute.org/events.php/589/asia-pacific-conference-2016>.

Mohanty, S., Ganguly, M. and Pattnaik, P.K., 2018. CIA Triad for Achieving Accountability in Cloud Computing Environment.

Murphy, J., (2017). We really don’t trust our government or institutions anymore. news.com.au, 22 Jan 2017.

Nandakumar, K., & Jain, A. K. (2015). Biometric Template Protection: Bridging the performance gap between theory and practice. Signal Processing Magazine, IEEE, 32(5), 88-100.

Nash, E. (2017). "Facial recognition to replace passports in radical security overhaul at Australian airports", TOTT News.

Osborne, P. (2016). Abbott backs national ID card: senator. The Australian, 19 Oct 2016.

O'Sullivan, M. (2017). " Sydney 2026 - The New Airport", Sydney Morning Hearld.

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable Biometrics: A review. Signal Processing Magazine, IEEE, 32(5), 54-65.

Ponterotto, J.G., (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. Journal of counseling psychology, 52(2), p.126.

Population Clock, Australian Bureau of Statistics website, viewed 19 Aug 2017, <http://abs.gov.au/AUSSTATS/abs@.nsf/Web+Pages/Population+Clock?opendocument>.

Quinn, L. (2015). Australia to become world's first country to trial cloud passport. Daily Mail Online, viewed 30 Apr 2016, <http://www.dailymail.co.uk/news/article-3294127/Australia-world-s-country-trial-travel-without-PASSPORT-Julie-Bishop-says-global.html>.

Raddon, A., (2010). Early stage research training: Epistemology & ontology in social science research. Generic Skills Training for Research Students.

Rauniar, R., Rawski, G., Yang, J. and Johnson, B., 2014. Technology acceptance model (TAM) and social media usage: an empirical study on Facebook. Journal of Enterprise Information Management, 27(1), pp.6-30.

Recker, J., (2012). Scientific research in information systems: a beginner's guide. Springer Science & Business Media.

Roberts, B., McGonegal, S., Prager, F., Wei, D., Rose, A.Z., Baschnagel, C., Beggs, T. and Baghelai, O., (2014). Analysis of primary inspection wait time at US ports of entry.

Rose, J. (2016). Biometrics as a Service: the next giant leap?. Biometric Technology Today, 2016(3), 7-9.

Saunders, M., Lewis, P. and Thornhill, A. (2015). Research methods for business students. 7th ed.

Schouten, B., & Jacobs, B. (2009). Biometrics and their use in e-passports. Image and Vision Computing, 27(3), 305-312.

Sendi, A.S. and Cheriet, M., 2014, March. Cloud computing: A risk assessment model. In Cloud Engineering (IC2E), 2014 IEEE International Conference on (pp. 147-152). IEEE.

Sharma, M. (2007). "SmartGate passport check goes national", The Weekend Australian.

Sharp, P. (2012). "World's First Commercial Airline - The Greatest Moments in Flight". Space.com website 19 Jul 2012, viewed 23 Apr 2017, <http://www.space.com/16657-worlds-first-commercial-airline-the-greatest-moments-in-flight.html>.

Smith, S. (2013). Determining Sample Size: How to Ensure You Get the Correct Sample Size, Qualtrics web site, viewed 31 Map 2017, <https://www.qualtrics.com/blog/determining-sample-size/>.

Spoiala, C. (2015), "Cloud offering: Comparison between IaaS, PaaS, SaaS, BaaS" (2015). Assist Software Romania, April 2015. <https://assist-software.net/blog/cloud-offering-comparison-between-iaas-paas-saas-baas>.

Srivastava, J.N., (2001). Science and Spirituality in the new millennium. Thoughts on the synthesis of Science and Religion"(Eds: TD Singh & S. Bandopadhyay) The Bhaktivedanta Institute, Kolkata, pp.580-593.

Stafford, A. (2007). Labor pledges to kill off Access Card. The age, 29 Aug 2007.

Stanford, C. (2016). Press Release: Gartner Says By 2020 a Corporate No-Cloud Policy Will Be as Rare as a No-Internet Policy Is Today, viewed 12 Oct 2016, <http://www.gartner.com/newsroom/id/3354117>.

Suren, M. (2010) Hybrid Cloud Solutions With Windows Azure AppFabric Middleware, Microsoft Developer Blog, viewed 30/10/2016, <https://blogs.msdn.microsoft.com/appfabriccat/2010/11/29/hybrid-cloud-solutions-with-windows-azure-appfabric-middleware/>

Thakkar, A. D. (2013). Implementation of identity as a service (IDaaS) provided by secure third party authentication server. (Doctoral dissertation, San Diego State University).

Thomas, M. V., & Chandrasekaran, K. (2016). Identity and Access Management in the Cloud Computing Environments. Developing Interoperable and Federated Cloud Architecture, 61.

Tiwari, P., Joshi, S., (2015). Data Security for Software as a Service. Web-Based Services: Concepts, Methodologies, Tools, and Applications, Ch 39.

Trochim William, M., (2006). Likert Scaling. Research Methods Knowledge Base,.

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern recognition, 47(8), 2673-2688.

Unisys Survey Finds Wearable Technology to Revolutionize Biometrics, Unisys 2016, viewed 12 Feb 2017, <http://http://www.unisys.com/offerings/security-solutions/News%20Release/unisys-survey-finds-wearable-tech-to-revolutionize-biometrics>.

Vallabhu, H. and Satyanarayana, R.V. (2012). Biometric authentication as a service on cloud: Novel solution. International Journal of Soft Computing and Engineering, 2(4), p.163.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D., 2003. User acceptance of information technology: Toward a unified view. MIS quarterly, pp.425-478.

Wallace, L.G. and Sheetz, S.D., 2014. The adoption of software measures: A technology acceptance model (TAM) perspective. Information & Management, 51(2), pp.249-259

White, D., Dunn, J.D., Schmid, A.C. and Kemp, R.I. (2015). Error rates in users of automatic face recognition software. PloS one, 10(10), p.e0139827.

White, D., Kemp, R.I., Jenkins, R., Matheson, M. and Burton, A.M., (2014). Passport officers' errors in face matching. PloS one, 9(8), p.e103510.

Williams, M.D., Rana, N.P. and Dwivedi, Y.K., 2015. The unified theory of acceptance and use of technology (UTAUT): a literature review. Journal of Enterprise Information Management, 28(3), pp.443-488.

Witty, R.J., Allan, A., Enck, J. and Wagner, R. (2003). Identity and access management defined. Research Study SPA-21-3430, Gartner.

Wu, R., Zhang, X., Ahn, G. J., Sharifi, H., & Xie, H. (2013). ACaaS: Access control as a service for IaaS cloud. In Social Computing (SocialCom), 2013 International Conference on (pp. 423-428). IEEE.

Zamawe, F. C. (2015). The Implication of Using NVivo Software in Qualitative Data Analysis: Evidence-Based Reflections. Malawi Medical Journal, 27(1), 13–15.

Appendix A - Approval letter of the survey by the Macquarie University Human Research Ethics Committee (HREC)

Dear Dr Busch

RE: Ethics project entitled: "Global Identification on the Cloud: Cloud Passport adoption"

Ref number: 5201600824

The Faculty of Science and Engineering Human Research Ethics Sub-Committee has reviewed your application and granted final approval, effective 10/01/2017. You may now commence your research.

This research meets the requirements of the National Statement on Ethical Conduct in Human Research (2007). The National Statement is available at the following web site:

http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72.pdf.

The following personnel are authorised to conduct this research:

Dr Peter Busch
Mr Tonnie Lam

NB. STUDENTS: IT IS YOUR RESPONSIBILITY TO KEEP A COPY OF THIS APPROVAL EMAIL TO SUBMIT WITH YOUR THESIS.

Please note the following standard requirements of approval:

1. The approval of this project is conditional upon your continuing compliance with the National Statement on Ethical Conduct in Human Research (2007).

2. Approval will be for a period of five (5) years subject to the provision of annual reports.

Progress Report 1 Due: 10/01/2018
Progress Report 2 Due: 10/01/2019
Progress Report 3 Due: 10/01/2020
Progress Report 4 Due: 10/01/2021
Final Report Due: 10/01/2022

NB. If you complete the work earlier than you had planned you must submit a Final Report as soon as the work is completed. If the project has been discontinued or not commenced for any reason, you are also required to submit a Final Report for the project.

Progress reports and Final Reports are available at the following website:

http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/forms

3. If the project has run for more than five (5) years you cannot renew approval for the project. You will need to complete and submit a Final Report and submit a new application for the project. (The five year limit on renewal of approvals allows the Committee to fully re-review research in an environment where legislation, guidelines and requirements are continually changing, for example, new child protection and privacy laws).

4. All amendments to the project must be reviewed and approved by the Committee before implementation. Please complete and submit a Request for Amendment Form available at the following website:

http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/forms

5. Please notify the Committee immediately in the event of any adverse effects on participants or of any unforeseen events that affect the continued ethical acceptability of the project.

6. At all times you are responsible for the ethical conduct of your research in accordance with the guidelines established by the University. This information is available at the following websites:
http://www.mq.edu.au/policy/

http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/policy

If you will be applying for or have applied for internal or external funding for the above project it is your responsibility to provide the Macquarie University's Research Grants Management Assistant with a copy of this email as soon as possible. Internal and External funding agencies will not be informed that you have final approval for your project and funds will not be released until the Research Grants Management Assistant has received a copy of this email.

If you need to provide a hard copy letter of Final Approval to an external organisation as evidence that you have Final Approval, please do not hesitate to contact the Ethics Secretariat at the address below.

Please retain a copy of this email as this is your official notification of final ethics approval.

Yours sincerely,
Human Research Ethics Sub-Committee
Faculty of Science and Engineering
Macquarie University
NSW 2109

Appendix B – Supplementary Materials for Chapter 1

Summary table of the Year-on-Year (YoY) increase of passengers handled by top 50 airports

Year	Total Number of Passengers	Average Number of Passengers	Year on Year (YoY) % Increase
2010	2,074,363,697	41,487,274	
2011	2,176,902,628	43,538,053	4.9%
2012	2,262,861,823	45,257,236	3.9%
2013	2,338,413,231	46,768,265	3.3%
2014	2,441,842,673	48,836,853	4.4%
2015	2,590,144,985	51,802,900	6.1%
2016	2,723,710,473	54,474,209	5.2%
Increase from 2010 to 2016			31.3%

Table B.1 - Year-on-Year (YoY) increase of passengers handled by top 50 airports (Source: Wikipedia 2017)

Top 10 Australian Airports by passenger movements, in thousands (Source: Airport Traffic Data 2017)

Rank	Airport	2010–11	2012-13	2014-15	2015-16
1	Sydney Airport	35,958	37,603	39,022	41,091
2	Melbourne Airport	27,963	29,492	31,936	33,705
3	Brisbane Airport	19,975	21,145	21,918	22,320
4	Perth Airport	10,890	12,832	12,730	12,558
5	Adelaide Airport	7,279	7,171	7,670	7,778
6	Gold Coast Airport	5,486	5,805	5,867	6,273
7	Cairns Airport	3,859	4,158	4,391	4,711
8	Canberra Airport	3,241	3,014	2,804	2,815
9	Hobart International Airport	1,903	2,027	2,186	2,313
10	Darwin International Airport	1,680	1,903	2,057	2,041

Table B.2 - Top 10 Australian Airports by passenger movements, in thousands (Source: Airport Traffic Data 2017)

Appendix C– Supplementary Materials for Chapter 2

Typical Cloud Typologies

The common cloud computing service models are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) (Baun, Kunze, Nimis & Tai 2011). The Australian government defines different types of service models in the Australian Government Cloud Computing Policy (2014 edition), as follows:

Software as a Service (SaaS) provides applications running on a cloud-based infrastructure. The applications are accessed through either a web browser or program interface. All underlying cloud infrastructure, network, storage and operating systems configurations and capabilities of application services are maintained by service providers.

Platform as a Service (PaaS) provides a cloud-based infrastructure for clients to deploy their own client-created or acquired applications, without the complexity of building and maintaining details of the components of the infrastructure. The underlying cloud infrastructure, network, storage and operating system configuration is maintained by service providers, while clients have control over their deployed applications and configuration settings.

Infrastructure as a Service (IaaS) provides a cloud-based infrastructure that is fully configurable by the clients to deploy their operating systems and applications. The underlying cloud infrastructure is still controlled by the service providers; however, clients have the control over operating systems, storage, and deployed applications, and possibly some networking components like host firewall settings.

Different types of Service-Oriented Architecture (SOA) for cloud computing are summarised in figure C.1 below. Within different types of service models of cloud computing, there are also different types of cloud architecture or deployment models for different types of the purpose of the business environment (Baun et al., 2011; Australian Government Cloud Computing Policy 2014).

Public cloud is a cloud infrastructure accessible to the general public. Usually, providers and potential clients do not belong to the same organisation. The physical infrastructure for the cloud service is independently maintained by the provider only. Because the cloud service is not owned or managed by a dedicated client, the services provided are billed based on resources used in the corresponding period.

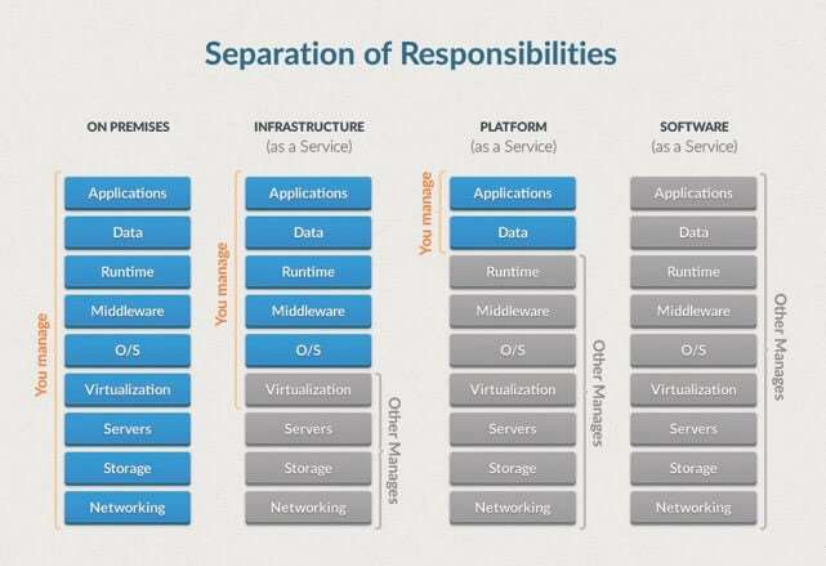


Figure C.1 - Cloud Services – Separation of Responsibilities (Source: Spoiala 2015)

A private cloud, on the contrary, is a cloud infrastructure, which is exclusively used by a single organisation, usually comprising multiple clients or business units. It is normally owned, managed, and operated by the organisation, and usually on the business premises. The main reason why a private cloud is used is mainly for security concerns. Business within the private cloud can have total control over the level of access of data based on the sensitivity of the information, for example on personal health data, against different kinds of users or organisations.

Hybrid cloud as the third kind of deployment model is a cloud infrastructure composed of partly public cloud and partly private cloud. The two sets of cloud architectures remain unique entities, but are bound together to act as a release control on data and application; this is particularly useful for load balancing during peak periods so that certain processes can offload to the public cloud while keeping the private cloud to run core functionalities.

A diagram to show different types of cloud architecture is shown in figure C.2 below. As cloud services providers specialise in particular types of applications and services, they will be the best parties to manage upgrades and maintenance, backups, disaster recovery, and fail-over functions for all clients that subscribe their cloud services. As a result, clients of cloud services may see increased reliability, even as costs decline due to economies of scale as well as other production factors (Jamil, Zaki 2011).

The following represents the main benefits of cloud computing for companies (Jamil, Zaki 2011):

- Reduced cost: cloud technology is charged as a pay-as-you-go service model, which helps companies to minimise unused resources, and hence saves costs
- Flexible storage and processing power: organisations can have an elastic model of CPU power as well as storage of business data in the cloud, which changes according to the

size and growth rate of the business, and without worrying about adding or removing servers or hard disks

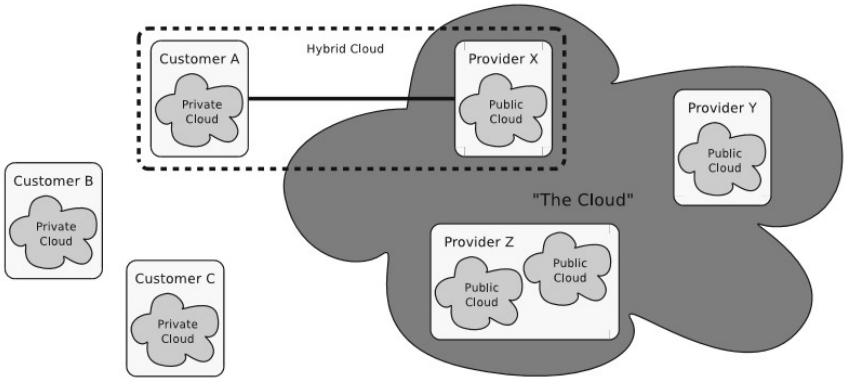


Figure C.2 - Public cloud, private cloud, and hybrid cloud (source: Baun et al., 2011)

- Automated system refresh: clients no longer need to worry about keeping software or hardware up to date, as it is handled by the cloud service providers automatically
- More mobility: users in business can access information wherever they are, rather than having to remain at their desks
- Allows IT to shift focus: as the business no longer having to worry about constant server updates and other infrastructure issues, IT department can concentrate on forward-looking projects, such as value-added innovation and strategic planning for future business

Amazon Elastic Compute Cloud (Amazon EC2) from Amazon Web Service (AWS)

The following are system management tools that AWS introduces for clients to harness IT resources:

- AWS Management Console: Resource control and monitoring

- AWS Billing and Cost Management: Resource billing and cost estimation

The AWS Management Console (Figure C.3) is a tool for clients to access and manage Amazon Web Services through a user-friendly web-based user interface. It enables clients to control the type and the volume of cloud resources for the organisation. According to AWS, clients can use the AWS Management Console to control cloud system sources such as the configuration of Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting Amazon CloudWatch alarms can be accessed and monitored from the AWS Management Console.

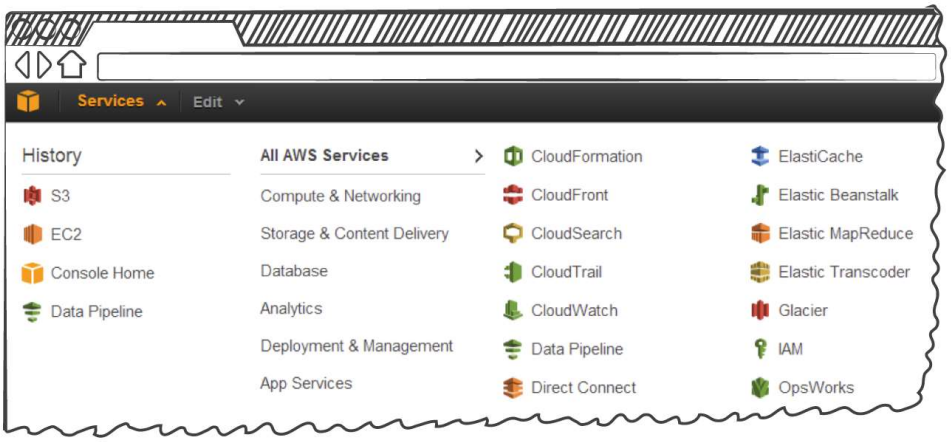


Figure C.3 - AWS Management Console (Working with the AWS Management Console AWS - Management Console 2016)

AWS Billing and Cost Management, on the other hand, is the service for clients to review and monitor usage level, as well as to estimate and plan AWS cost budgets. Apart from having a vast set of tools and graphs to analysis billing charges for clients, AWS Billing and Cost Management provide a dashboard-based cost visualisation function (see figure C.4 below) to perform forecasts of costs from selected cloud resources. Clients can use Amazon CloudWatch to create billing alerts to clients whenever AWS costs exceed specified thresholds. Same cases can be done on cost estimation, as CloudWatch can also be used to notify clients when budgeted amounts or estimated costs exceed estimated budgets.

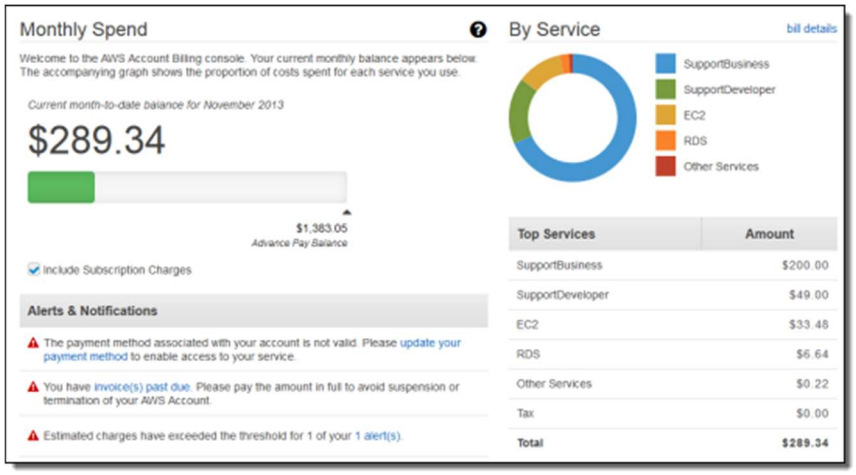


Figure C.4 - AWS Billing and Cost Management Dashboard (AWS Billing and Cost Management - User Guide 2016)

Appendix D - Details on the Setup of Facebook Advertising Campaign for the Survey

An example and location of the advertisement on the Facebook web page are shown in the figures below.

Figure D.1 – Appearance of the Facebook advertisement for the survey

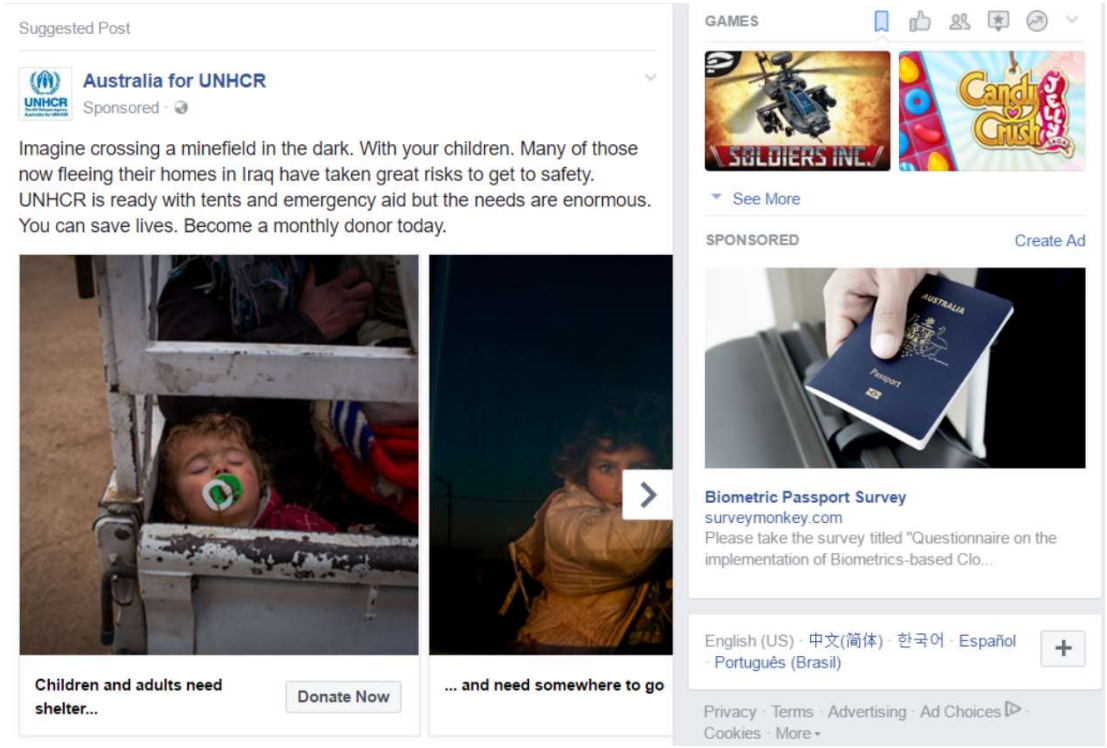


Figure D.2 – Location of the advertisement for the survey on the Facebook page

The Facebook advertising campaign is set to reach all adult Australian users, by configuring the advertisement parameters in the following settings:

- For the type of advertising campaign on Facebook for the nature of the current research, the method to draw user's attention and increase traffic to the online survey link on www.surveymonkey.com was chosen.
- Then a certain amount of budget for the campaign was selected for each day, and a total amount for the whole Facebook advertising campaign was set.
- For the audience type, the campaign was set up to target for English-speaking male and female Australian Facebook users in all states, with age of 18 and above.
- For the placement type within the Facebook page, which defines the platforms and location on the web page where the advertisement is to be placed, the platform for desktop only and the location of the Facebook ad at the sidebar was chosen for the current survey campaign.

Appendix E – Questionnaire for the Cloud Passport Survey

MACQUARIE University
SYDNEY·AUSTRALIA

Questionnaire on the implementation of Biometrics-based Cloud Passport in Australia

Participant information and Consent Form

Name of Project: Global Identification on the Cloud: a study of ideas and development of Cloud Passport Adoption

You are invited to participate in a study to find out the attitudes of the general public on the vision of Cloud passport as an alternative for the current travel document arrangement.

The purpose of the study is through interviews and questionnaire surveys to find out the attitudes of the general public on the acceptance of the idea of Cloud Passport. Based on collected data, this research will report social phenomena on the human aspects of the perception of Cloud Passport, and providing analysis and interpretation for a possible successful implementation of Cloud Passport in the future.

The research is being conducted by Tonnie Lam (yuk-tung.lam@students.mq.edu.au) to meet the requirements of the second year of his Master of Research degree under the supervision of Dr Peter Busch (peter.busch@mq.edu.au x9520) of the Department of Computing.

If you decide to participate, you will be asked to undertake a questionnaire that asks about:

- Basic demographic information (gender, age range, education level & occupation type)
- the level of acceptance of the concept of Cloud Passport (travel to other countries without the need to physical passport) as a future method
- the attitude towards the way to deal with machines rather than people in border control
- the degree of concern on having biometrics information (face, fingerprints as examples) stored in the cloud as the identification method for Cloud Passport
- General comments on the survey topic

There is no remuneration for participating in the questionnaire, and the questionnaire should take about 10-15 minutes to complete.

Any information or personal details gathered in the course of the study are confidential, except as required by law. No individual will be identified in any publication of the results. Only the researchers Dr Peter Busch and Tonnie Lam will have access to the research results. A summary of the results of the data can be made available to you on request by contacting Dr Peter Busch. It is possible that we may use the de-identified data for use in future Human Research Ethics Committee-approved projects.

Participation in this study is entirely voluntary: you are not obliged to participate and if you decide to participate, you are free to withdraw at any time without having to give a reason and without consequence.

The ethical aspects of this study have been approved by the Macquarie University Human Research Ethics Committee. If you have any complaints or reservations about any ethical aspect of your participation in this research, you may contact the Committee through the Director, Research Ethics & Integrity (telephone (02) 9850 7854; email ethics@mq.edu.au). Any complaint you make will be treated in confidence and investigated, and you will be informed of the outcome. Please feel free to print a copy of this consent page to keep for your records.

* 1. By choosing "Yes" below indicates that you are 18 years of age or older, and indicates your consent to participate in this survey.

- ◯ Yes
- ◯ No

Introduction

The aim of this survey is for academic research into the implementation of Cloud Passports, an award-winning initiative by the Australian federal government which enables travellers to travel to certain countries without the need of a physical travel document.

In the Cloud passport initiative, the current physical passports are proposed to be replaced by digital versions. The proposed new cloud passport has the following properties:

- Travellers will be authenticated by their biometrics features (face, fingerprint, iris etc.) when they pass through the automatic border gate (e.g. SmartGate in Australia & NZ)
- Biometrics information of travellers are strongly encrypted and stored securely in government's server
- Biometrics information of travellers will make available to other countries through a secure cloud-based communication link
- Travellers do not need to have a physical travel document, as their identity will be authenticated by their biometrics information supply by their country of origin

Benefits of the proposed Cloud Passport are:

- Increased throughput to handle more travellers to pass the border gate at less cost
- Reduced waiting and queueing time of travellers in passing the border gate
- Reduced cost for producing and reissuing physical passports
- Eliminate the possibility of losing physical passports
- Reduce the error rate in the identification process through replacing human factors with a complex computer-based recognition mechanism
- Better level of surveillance in preventing terrorists or extremists from moving between countries

The initial scope of the proposed Cloud Passport implementation is for citizens of Australia and New Zealand when they travel between the two countries. If the implementation of Cloud Passport between the two countries is successful, then other countries may be invited to join in.

Start of Survey

2. What is your state of residence in Australia?

- ◯ Australian Capital Territory
- ◯ New South Wales
- ◯ Northern Territory
- ◯ Queensland
- ◯ South Australia
- ◯ Tasmania
- ◯ Victoria
- ◯ Western Australia

3. What is your gender?

- ◯ Male
- ◯ Female
- ◯ Prefer not to answer

4. What is your age?

- ◯ 18-25 years old
- ◯ 26-35 years old
- ◯ 36-49 years old
- ◯ 50-65 years old
- ◯ Over 65 years old
- ◯ Prefer not to answer

5. What is the highest degree or level of school you have completed?

- ◯ Less than Year 12 or equivalent
- ◯ Year 12 or equivalent (HSC/Leaving cert)
- ◯ Vocational Qualification
- ◯ Associate diploma / Undergraduate diploma
- ◯ Bachelor degree (including honours)
- ◯ Postgraduate diploma (includes graduate diploma)
- ◯ Master's degree
- ◯ Doctorate
- ◯ Prefer not to answer

6. Which of the following most closely matches your job title?

- ◯ Unemployed / Retired
- ◯ Student
- ◯ Junior / Entry level
- ◯ Professional level
- ◯ Managerial level
- ◯ Senior Manager / C-level executives (CEO, CFO, CIO, COO etc.)
- ◯ Business Owner / Entrepreneur
- ◯ Other (please specify)

7. Do you have a passport (travel document)?

- ◯ Yes
- ◯ No

8. If yes, which country or region is your passport issued?

- ◯ Australia / New Zealand
- ◯ United Kingdom
- ◯ India
- ◯ China
- ◯ South-east Asian Countries
- ◯ Other Asia-Pacific Countries
- ◯ European Countries
- ◯ North American Countries
- ◯ Central and South American Countries
- ◯ African Countries
- ◯ Other (please specify)

9. How frequently do you travel overseas per year?

- ◯ Zero
- ◯ 1-2 times
- ◯ 3-5 times
- ◯ 6-10 times
- ◯ > 10 times

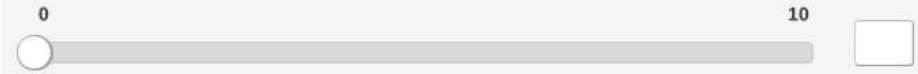
10. Which country or region in the world have you travelled before, or intend to travel to in the future? (Can choose one or more options)

- ☐ New Zealand
- ☐ United Kingdom
- ☐ India
- ☐ China
- ☐ South-east Asian Countries
- ☐ Other Asia-Pacific Countries
- ☐ European Countries
- ☐ North American Countries
- ☐ Central and South American Countries
- ☐ African Countries
- ☐ Other (please specify)

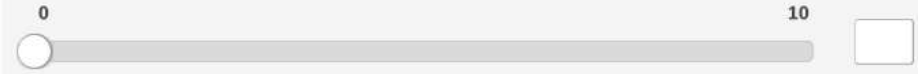
11. What is the main reason for travelling overseas?

- ◯ Business
- ◯ Leisure
- ◯ Other (please specify)

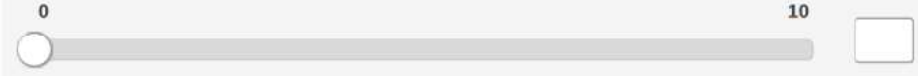
12. Do you favour on the idea of Cloud Passport, which identifies travellers by biometric information (such as facial recognition, fingerprints, iris), without the need of a physical passport (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?



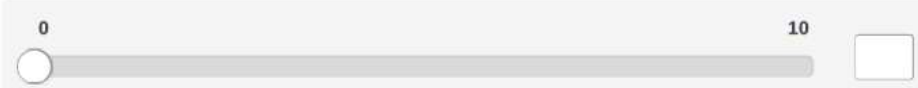
13. Do you favour on replacing most of the government personnel with automatic border gates when passing through border control in the airport (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?



14. Do you favour on the use of one or more biometric features (face, fingerprint, iris etc.) to verify the identity of a traveller (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour)?



15. Do you favour on the idea of storing traveller's biometrics features (face, fingerprint, iris etc.) in a government database, and make available to other countries through a secure cloud-based communication link (select a rating of 1 to 10, 1 – least favour to 10 – strongly favour) ?



16. Do you think the concept of Cloud Passport will be widely used in countries around the world in the next 10 – 20 years?

- ◯ Yes
- ◯ No

17. Any other comments on the survey?