Cloud Computing Security and Forensics Issues and Awareness of Cloud Storage Users in Malaysia

Yee Say Keat¹, Babak Bashari Rad², Mohammad Ahmadi³
School of Computing and Technology
Asia Pacific University of Technology & Innovation (APU)
Technology Park Malaysia (TPM), Bukit Jalil, Kuala Lumpur 57000 Malaysia
¹ adamyeeere@gmail.com, ² babak.basharirad@apu.edu.my, ³ ahmadi@apu.edu.my

ABSTRACT

Cloud storage services are widely getting acceptance and gaining popularity, since it is used mostly by companies and students in Malaysian higher learning institutions. While cloud storage services got popular within last two years, most of the people are still trying to adapt to this new technology and some people still does not fully understand what cloud storage services are. In this paper, the authors present the results and an analysis of survey conducted on the awareness and concerns of Malaysians about cloud storage services, and its forensics and security issues. Questionnaires were administered to two hundred fifty users of cloud storage in Malaysia and fifty to the public to get the responses of people, especially student concerning about the cloud storage services. The responses from participants revealed valuable information about the public awareness and knowledge on cloud services. Relevant areas that required improvements are also investigated and discussed in this paper.

KEYWORDS
Cloud Computing, Cloud Forensics, Cloud Security, Forensics Awareness

1 INTRODUCTION

Cloud storage services are increasingly used by various types of ordinary consumers and professional businesses, as well as government departments and organizations that might store large amount of data, such as educational institutions [1]. The new trend in storing data is to use cloud storage, due to its convenience and accessibility, anytime, and anywhere [2]. There are still many problems and concerns for cloud storages [3]. For example, if the security of the cloud storage system has compromised, can cloud storage administrators or investigation officers view users’ confidential data and what would be the best way to prevent that from view? A survey has been conducted from the users of cloud storage services and white-collar users from the Information Technology and business based industries to explore these concerns. The study involves data collection among students in several universities in Malaysia using questionnaires. The authors believe this research would help investigators, examiners and developers or forensic investigation companies who are interested in developing forensics tools, countermeasures, and techniques to develop their knowledge and skills of investigations based on the public consciousness of cloud storage in Malaysia.

2 LITERATURE REVIEW

Cloud storage forensic research is considered as a new research area and hot topic in information technology [4] [5]. As people are trying to adapt to this new technology and service, most of people are also trying to gain more information and knowledge on what this new technology can offer [6]. Furthermore, as more people use the cloud storage services, the more dangerous issues and challenges it will present for security and forensic investigators [7]. This is because cloud storage services are open to anyone who has access to the Internet. Users such as hackers are also welcome to use the services to conduct any crime activities [8] [9]. The group of hackers will find any of the systems vulnerabilities and conduct the hacking activities. For example, the incident about Apple in year of 2014, around 26 various celebrities’ naked photo had been taken by the group of hackers [10]. Furthermore, Cloud computing is computing based on the internet. Last 10-20 years, people would run applications or programs from software downloaded on a physical computer or place
servers inside their organizations. However, nowadays, cloud computing technology allows users to access to the same kinds of programs and platform through the internet [11].

2.1 Introduction to the “Cloud”

Before the discussion forensic starts with the cloud computing, the researcher would like to talk about what is this “cloud” that most of the people keep talking or the topic that everyone chatting about. So, the researcher found that the best way to discuss and understand the “Cloud” is to go back to 5 years or even 10 years ago, record back the day that how you stored all of your data, your music, your photos and your files. All of us have been through that period, it used to be the period that all of us stored our personal data on a physical piece of hardware like hard disk, pen drive, or CD or even stored on a floppy disk in 1990s year. Furthermore, in the most basic terms to define “Cloud”, it refers to the internet at all times. Some of the cloud engineers might shout at those people for being that basic, but the fact is that internet connection is a must for cloud services to work [12]. Therefore, someone will say, “I stored my data in the Cloud”, it means they have stored their data on an internet service. For example, email services are definitely provided through internet and in “The Cloud”. Moreover, another good definition of “Cloud” is you might be listening to music on a music service provider like Spotify or you might be looking photo on Facebook and watching movie on Netflix. If you are doing any activities that the research mentioned, the music, movies, and photos are not on your personal computer, it is all in somewhere else and that place is called “The Cloud”.

On the other hand, of course at the moment “cloud” is not that really simple and easy term anymore. The term “Cloud” or cloud computing are referring to an application or a service provider that is hosted by a company or run through internet servers [13]. In addition, Google, Apple, Facebook and Yahoo have their own servers or server farms. For example, in North Carolina, Apple even built a huge server farm for his own cloud service- iCloud [14]. In this paper, the researcher adopts the definition of cloud computing and discuss the digital forensic process in order to complete the comparison of cloud storage computing at the end of the project.

2.2 Introduction to Cloud Computing

Cloud computing is transforming the way information technology is managed and consumed, improvements in cost efficiencies, accelerated technology and innovation, and the ability to scope applications on demand [15]. Cloud computing is a model for an on-demand network access to a shared pool of configurable computing resources and it can minimize management efforts or interaction of service provider [16]. For example, servers, networks, storage, services and applications carrying conveniently and rapidly provisioned. In a very simple definition for cloud computing, it is a combination of technology, which present a platform to provide hosting and storage services through the internet [17]. Furthermore, cloud computing is referring the high-end of information technology for society, so the main objectives for cloud computing is to produce and offer a standard service, with low cost on-demand computing infrastructure by providing a satisfactory resource, quality and stability of service levels [18]. At this moment, there are many companies who provide offering and developing cloud computing services and products but they are lack in considered the accessing and storing data in a shared and virtualized environment properly. Thus, most of the expert cloud-based application developers are struggling to include security due to the current affordable technology capabilities which cause trouble to the cloud computing providers because they should make sure their service is safe enough from all of the external threats [19]. On the other hand, the benefits of cloud computing are tremendous and one of the strongest and important benefit is the cloud computing users do not need to purchase the resources from a third party vendor, instead, they can just use the resources which exist in the market and just pay for it as a service thus help the customers to reduce money and time consumed.

Furthermore, not obvious when the word of “cloud computing” was first created in the market. For example, several experts and people
proposed that “cloud computing” term was properly stated and introduced by Eric Schmidt, the Chief Executive of Google Company in 2016 [20]. In addition, according to Kaufman in 2009 has suggested the term of “cloud computing” was originated from the telecommunications environment in 1990s, when everyone and included the providers has begun to use virtual private network (VPN) services for data communication [21]. Adoption of cloud computing has been a marked increase recent years [22]. There was a research which sponsored by The Microsoft forecasted the “Cloud IT services” spent on public in 2011 year was twenty-eight billion USD compared with more than one trillion seven hundred billion USD in an entire spending on IT services and products. Hence, this shows that it slowly transforming IT provides economic value to most of the countries, town, small business, big business, and industries [22]. The importance of cloud storage services is that they are becoming prevalent choices for public and society to store data that is accessible via a range of devices such as smartphones, personal computers (PC), laptops, and tables. Additionally, a lot of cloud storage practitioners do provide the services to the public and these companies also offer free capacity of cloud storage services, the cloud storage service practitioners are Google Drive, Microsoft- SkyDrive and Dropbox [23].

2.3 Cloud Computing Security and Issues

The security and privacy issues will always be a topic of concern. In 21st century, all of us are living in an increasingly interconnected environment, from social-network to personal banking and to government infrastructure, and protecting the networks are no longer optional for consideration [24]. There are multiple security issues for cloud computing as it surrounds a lot of technologies including operating systems, virtualization, database, transaction management and the most important technology at the moment- network [25]. Hence, cloud computing contains security issues for most of these applicable technologies and systems [26]. For example, network that interconnects the systems in the cloud must be secured enough in order to avoid security and privacy issues happen in those systems or mapping the physical machines to the virtual machines have to be carried out securely [27]. On the other hand, data stored in the cloud computing is very important as data protection involving data encryption as well as assuring suitable policies are implement or data sharing of enforcement [28]. You might be wondering what data is or why it is very important. Data is a collection of facts and information that have been translated, gathered, and collected for some purpose usually for analysis [29]. Additionally, it can be any character including pictures, charts, sound and video and number and text [30]. Thus, why data is so important? This is because data includes your personal data, transaction data, or business data (customer data) which must be kept secret and cannot be revealed to unauthorized person [30]. No matter what kind of data it is, all of the data needs to be processed, collected, generated and someone has to usually be a data scientist. In the 21st century, data scientists are the most sought after positions. According to ex-exec at Google, Google claimed that data scientist is the “sexiest job of the 21st century” [31]. In addition, another example for important of data is according to Minister of Higher Education Malaysia indicate that will have 12,000 Big Data scientists are needed within the next five years to spur and drive Malaysia’s data –driven economy. So, this shows that how important the data is and how important the data scientists play the role in 21st century.

For security purpose, the cryptographic encryption mechanisms are definitely the best choices because hard-core manufacturers are now shipping self-encryption transmission and built encryption hardware into drive and offering automated encryption with performance collision [32]. Thus, encryption key is hardly to steal and it is very hard or nearly impossible for anyone even hackers themselves to decrypted the encrypted key [33]. Furthermore, the best choice of encryption for protecting data. The integrity and authentication protection mechanisms will ensure that the data only goes wherever customers want and it will not have transit modifying [34]. In addition, user authentication is the priority and basis for access control. In the cloud computing environment all of the data are accessible to everyone through the internet, the access control and
authentication are very important than ever since the cloud [35]. Therefore, having a strong authentication is mandatory and compulsory requirements for any cloud computing development.

In cloud computing, legal, regulation, privacy issues are extremely important. It is very important to know and verify on cloud service provider’s legal, regulation and how well they protect and address the privacy issues [36]. Every customer must have its knowledge’s experts to examine cloud service provider’s practices and policies to ensure their sufficiency [37]. Most of the customer would like to choose a trusted platform and trusted cloud storage service because module access techniques play a very important part as a key task in set a limit to those sensitive and critical data in the areas of data retention and deletion. Therefore, just like what the researcher has mentioned early [38]. The cloud computing services are not fully protected, fully trusted and guarantee nothing will happen from being hacked. Customers need to have part of expecting the unexpected when they store their important data like photos or documentary in the cloud storage services, plan for the possibility of cloud provider’s protection might been hacked or data might have been breached to the society or sometime by users themselves in misbehaviour for using a cloud storage services [39]. For example, in 2014 year, which was two years ago from now [40]. A collection of almost 500 private photos of various celebrities (mostly female celebrity with contain nudity) have been obtained through a break of Apple’s cloud storage service- iCloud [41]. Even though Apple provides the best cloud storage service (iCloud) but a group of hackers still successfully hacked and accessed to user account by taking advantage of a security issue in the iCloud API, which allowed hackers to make unlimited attempts and overt of guessing victims’ passwords [42].

2.4 Security Issues

Does the scenery of threats to privacy and security transform as organizations distract to cloud based systems, application, service, and storage? The new vectors are being introduced and old ones still be applied in the new methods [43]. It is important to admit that many of the cloud architectures can reduce and deny some of the current security and threat issues before categorizing the new threats [44]. A standardized interface can make the security management easier; many parties can generate more information for better security threat monitoring and evaluation [45]. For example, if data are still kept in the cloud, a loss of pilfer laptops or smartphones are much less likely to put sensitive, important, confidential and personal information at risk because a cloud storage service needs password to do the future actions. Therefore, some IT professionals with limited security experience and some of the user also very lack in security knowledge [46]. Hence, a good centralized security management and monitoring can be more effective for them because if they lack in security knowledge, they still believe in centralized and standardized cloud storage [46]. Furthermore, the mechanism of control can be attacked, breaking down isolation itself between users and allowing another user to access resources and data potentially when the network resources are being built on platforms, interfaces and systems that will share with others, another set of threat vectors are introduced in the meantime [47]. In addition, sometime the cloud-shared architecture also puts a cloud service user at the risk from other cloud user if users themselves with their bad behaviour draw attention from either bad media publicity or law enforcement [48]. Moreover, in a traditional architecture, personal computers inside the organizations may be at risk of compromises throughout a host of attack vectors utilizing some local applications such as documents viewers or internet browsers [49]. Some of the hackers can compromise credentials to gain and get access to the user’s cloud computer (cloud storage service) privileges and permissions even though the less data has been stored locally [43]. A compromise to the whole Gmail’s database might just begin with a compromised personal computer [49]. One of the examples, an attack has happened in year 2009 on the management team of Twitter Company. A compromised email password led to expose of a huge range of other very important data in other infrastructures of cloud [50]. Thus, sharing the tokens of
authentication can lead to fragile or brittle the wall of defences. Even without the benefits and advantages of cloud computing, the organization still must be careful to the important data (safeguard data) of the company as the data move around in the organization [50]. If an organization do not clean and delete the unnecessary data properly, the risk leaking privacy and sensitive data to outside will happen. Therefore, when depending to cloud storage service to handle data tasks and adequate security management practices must be priority and apposite care must be arranged such as encryption data and suitable deletion for some unnecessary things [51].

2.5 Type of Threats in Cloud Computing

The security issues and threats challenges are confronting by the group of organization who are hoping to use cloud storage services are not basically different from those subordinate on their home based managed enterprises [38]. Furthermore, the threats to information assets in the cloud be changed just based on the cloud delivery models that used by group of cloud user organizations. Few types of security threats as vulnerable facing to the cloud computing. In table 2, it provides a general picture of the security threats for cloud computing users and been categorized according to the Confidentiality, Integrity and Availability (CIA) security model and their relationship to each of the cloud service delivery model [36].

2.6 Type of Attackers/Hackers in Cloud Computing

The attackers can be divided into two groups of people that in each of the cloud computing service delivery models’ threats result. In table 3, type of attackers for internal and external will be discussed [43]. Even though attackers from internal and external able to define and differentiate clearly. The ability had to execute or hack successful attacks based on difference between them as threat to customer (user) and vendors same [52]. Furthermore, in the cloud computing world, hackers can be categorized in four types: random, weak, strong and substantial [53]. Every category is based on the capability to instigate or abet a successful attack rather than the type of threat they have presented.

- **Random**- The very general type of attacker that utilizing the simple and techniques tools. The attacker just scanned thought the internet randomly in order to search some vulnerable components, which can be hacked. Additionally, the attacker will deploy well known tools and techniques that can be detected easily.

- **Weak**- Attacker with a semi-skilled are targeting specific server and cloud computing providers by customizing existing public available techniques and tools or on specific targets. The semi-skilled attacker attempt to customize their attackers using available exploit and utilize tools and techniques.

- **Strong**- The skillful group of attackers, which might be a well organized crime group specializing in large and huge scope attacks. They will an internal and external hierarchy specializing on targeting particular or specific systems and applications and also the users of the cloud computing service.

- **Substantial**- The very strong group of attackers, they are requiring greater intelligence and skillful of knowledge on attacks and specialist resources in response to detection of an incident or security. A powerful attacker will not easily be detected by any parties or even by the organizations that they conducting the attack.
Table 1: The Security Threats for Cloud Computing [36]

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
</tr>
<tr>
<td>Insider user threats:</td>
<td>The insider’s user threats are to access user data held within the cloud storage is bigger as every of the models delivery which able to introduce the demands for many internal users as below: SaaS- cloud storage user and administration pf provider. PaaS- testing environment management and applications or systems developers IaaS- Third party platform consultations.</td>
</tr>
<tr>
<td>Malicious cloud service provider user</td>
<td></td>
</tr>
<tr>
<td>Malicious cloud service customer user</td>
<td></td>
</tr>
<tr>
<td>Malicious cloud service third party user (Support the could service provider or customer’s organizations)</td>
<td></td>
</tr>
<tr>
<td>External attacker/hacker threats:</td>
<td>The threat from external hackers just like attackers to any system. It perception to apply more to public internet face cloud computing. However, cloud storage where user endpoints can be targeted and all of the cloud delivery models are affected by external hackers especially in private cloud storage. Furthermore, cloud computing practitioners with huge data places that preserve details of credit card, confidential information, personal and privacy information or sensitive government policies or intellectual property will be leaded to attacks from groups. They will have major resources in order attempting or trying to retrieve and hack data. Hacking attack are also includes the threat of hardware and software attack, social engineering and supply chain attacks by expert professional specialized hackers (attackers).</td>
</tr>
<tr>
<td>Social engineering of cloud computing provider users and cloud storage users</td>
<td></td>
</tr>
<tr>
<td>Remote software attack of cloud systems or applications</td>
<td></td>
</tr>
<tr>
<td>Remote software attack of cloud infrastructure</td>
<td></td>
</tr>
<tr>
<td>Remote hardware attack against the cloud computing</td>
<td></td>
</tr>
<tr>
<td>Leakage of Data:</td>
<td>This is a threat from wide-ranging or extensive data leakage amongst others like potentially rival organizations also using the same cloud computing storage provider, which can be easily caused by human error, or incomplete hardware that will lead to data information compromise.</td>
</tr>
<tr>
<td>Security failure to access right across multiple domains</td>
<td></td>
</tr>
<tr>
<td>Electronic failure and physical transport systems for cloud computing backup and data</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td></td>
</tr>
<tr>
<td>Segregation of Data:</td>
<td>If resources of systems are effectively segregated SaaS as cloud hosting environment configured to share computing resource could provide a threat against data integrity.</td>
</tr>
<tr>
<td>Security perimeters were defined incorrectly.</td>
<td></td>
</tr>
<tr>
<td>Configuration of virtual machines (VM) and hypervisors are incorrect.</td>
<td></td>
</tr>
<tr>
<td>User access:</td>
<td>Implementation of poor access control processes creates a lot of threat opportunities. For example, a disaffected or disgruntled ex-employee of cloud provider company maintains remote access to organization administration customer cloud services and can lead to international damage to their data resources.</td>
</tr>
<tr>
<td>Poor access and identity management processes.</td>
<td></td>
</tr>
<tr>
<td>Quality of data:</td>
<td>The threat of collision quality of data is increased as cloud storage providers host much kind of customer’s data. The faulty, malfunction or incomplete component required by other cloud users can become potentially collision the data integrity for other cloud storage users that sharing the infrastructure.</td>
</tr>
<tr>
<td>Introduction of malfunction or incomplete application or infrastructure components.</td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
</tr>
<tr>
<td>Change management:</td>
<td>There is a threat that could change cloud computing introduce negative effects since the cloud computing provider increasing the responsibility for change management for all of the cloud delivery models.</td>
</tr>
<tr>
<td>Penetration of user testing will impact other cloud storage users.</td>
<td></td>
</tr>
<tr>
<td>The changes of infrastructure on cloud service provider, user/customer and third party systems will collision cloud computing users.</td>
<td></td>
</tr>
<tr>
<td>Denial of service threat:</td>
<td>The threat for denial of service will against the available cloud computing resources that are generally a threat comes from external to against public cloud services. Therefore, that can also impact all of the cloud service models as internal and external threat agents can be introduced hardware or application components that happen a denial of service.</td>
</tr>
<tr>
<td>Distributed of service for network bandwidth.</td>
<td></td>
</tr>
<tr>
<td>Denial of service for network DNS.</td>
<td></td>
</tr>
<tr>
<td>Denial of service for data and applications.</td>
<td></td>
</tr>
</tbody>
</table>
Table 2: Internal Attackers and External Attackers [43]

<table>
<thead>
<tr>
<th>Attackers from internal</th>
<th>Characteristics for an internal attacker/hacker:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓ The person is the cloud service practitioners, customer (user) or other provider from third party employee that performs their skill to support and manage the operation of a cloud services.</td>
</tr>
<tr>
<td></td>
<td>✓ Has the authorized to access to cloud computing services, supporting and managing infrastructure and systems or customer data. However, the legal authorized must be followed on their organizational rules and regulations.</td>
</tr>
<tr>
<td></td>
<td>✓ Using privileges or permission to gain more support or access third parties in executing attack against the privacy confidentiality integrity or the data (information) in the cloud service</td>
</tr>
<tr>
<td>Attackers from external</td>
<td>Characteristics for an external attacker/hacker:</td>
</tr>
<tr>
<td></td>
<td>✓ The person is not the cloud service provider, customer (user), other third party provider employee, or being employed by any parties that performs their skill to support and manage the operation of a cloud services.</td>
</tr>
<tr>
<td></td>
<td>✓ Has no the authorized to access to cloud computing services, supporting and managing infrastructure and applications or customer data.</td>
</tr>
<tr>
<td></td>
<td>✓ Expert to take advantages in operational, technical, procedures and social engineering vulnerabilities to attack a cloud computing service provider, customer (user) or third parties that support and manage organization to gain more access to spread attacks against the CIA which are confidentiality integrity and availability of data information among the cloud service.</td>
</tr>
</tbody>
</table>

3 AIM of the RESEARCH

The main aim of this research is to analyse and identify the level of awareness of cloud storage services among the normal users, as well as users from the white-collar organizations in Malaysia. This is to present awareness of Malaysians in cloud storage services that needs further understanding of security issues surrounding cloud storage and suggest improvements for people who are using these services. In order to achieve the aim of this research, the information was gathered by using a set of questionnaires, which are given to the respondents directly and with the aim of the questions being clearly stated.

4 DATA COLLECTION

Data were collected for this research using questionnaire, sent to respondents directly to get the most relevant and helpful information. Questionnaire also can bring many benefits such as receive public view, comments, thoughts, and opinions in very efficient way. In this study, the questionnaire has been produced using Google Form, as researchers found that most of the people would like to use this template to reply to survey because it is very easy to accomplish. Ten questions were developed by the researchers and divided into three segments: cloud computing, cloud forensics and cloud storage security and future expectations in cloud storage. However, the questions were developed and created to get important information in order to achieve the aim of this paper.

5 SAMPLING METHODS

Stratified sampling is employed to target populations in Malaysia. This method enables the division of targeted population into important different categories. However, this research mainly focused on the cloud storage forensic and security users. In addition, the researchers worked out the proportions needed for the sample to be the representative of this study. They also identified the different types of users as the target population. Therefore, the researchers divided the relative percentages of each group from the survey to make the results more accurate. The differentiation of major education background for cloud storage services’ users will have the different point of view of cloud storage forensic and security issues. This is the target population from a total of two hundred fifty users of cloud storage services in this study on the acceptance by the respondents, Information Technology: 55 students, Forensic and Security Computing: 75 students, Software Engineering: 40 students, Business Administration: 40 students, Mobile Technology: 20 and others: 20 students. In addition, fifty white collar from industry respondents are also participated in this research. Therefore, a total of three hundred cloud storage services’ users were participated in this research.
6 FINDINGS and ANALYSIS

This section will focus on the findings and analysis of data, which are collected by the authors via questionnaire. In addition, the data for this research will be presented and analysed using diagrams and figures.

6.1 Demographic Distribution of Respondents

The distribution of respondents in the study is shown in Figure 1. It demonstrates the education background of respondents as follows: Information Technology students: 18%, Forensic and Security Computing students: 25%, Software Engineering students: 13%, Business Administration students: 13%, Mobile Technology students 7% and others- 7%. In addition, 17% of the respondents are white-collar workers from the Information Technology, security, and business industries.

6.2 Respondents Perception of Cloud Computing in Malaysia

In this question, the researchers surveyed respondents on the perception and understandings of cloud computing as a trend in Malaysia. The questions were designed using a five Likert scale, which are strongly agree, agree, neutral, disagree and strongly disagree.

6.2.1 Cloud Computing as a Trend

The purpose of this question is to analyse respondent’s thought for cloud computing at the moment as the cloud computing technology is growing fast. Figure 2 demonstrates the responses’ thought of cloud computing as a trend at the moment in Malaysia. 300 respondents answered the question, the majority of respondents (75%) were strongly agree and agree that cloud computing at the moment in Malaysia is “a part of the evolving and growing process since the early years of computing”. 20% of respondents strongly agree or agree that cloud computing is a trend to “compromising security and reducing cost”. Only 5% of participants strongly agree and agree that cloud computing is just a “result of the recession for reducing information technology cost”. So, according to the result, the researchers would be able to know that the cost reduction is not the priority drive for cloud adoption. According to the result, 75% of respondents believe that the cloud computing is an evolving and evolution process of computing. As the very basic knowledge of Information Technology, IT growing and changing quickly, because the environment has changed [54]. For example, a sales person must be carrying as many documents as he can, to meet the customers 20 years ago. However, today he just need a tablet or a smartphone to go through all of the necessary documents and those documents are stored in cloud storage. IT has become the priority for everyone nowadays and it is also changing the life style of human beings [55]. This is what 75% of participants’ thoughts of cloud computing as it may change the way people storing the data.

Figure 1: Education Background
6.3 Cloud Storage Service’s Security

At the moment, most of the information technology users do not concern about the new technology that is being introduced to the market, but the users are concerning about the security of the technology [56]. According to Figure 3, 77% of the respondents are not interested in keeping their confidential data and private information in the cloud storage services, because not enough confident that any actions from the security department can be taken after the incident. Therefore, the majority of respondents believe cloud storage is not enough safe to store their personal information there. Only 23% of respondents do not fear to place their personal belongings like photos and videos in cloud storage, and agree that cloud storage services are secure places to preserve their private data. On the other hand, even though Malaysia has no serious security breach issues, like data breach or photos breach from the cloud storage services [57], but, the majority of the cloud storages’ users do not trust the cloud storages and do not keep their personal information and documents there, instead store their significant data in their personal hard disks or pen-drive and keep it all the time with them. Furthermore, the minority of 23% of participants believe in cloud storage services’ providers are able to provide a secure place for users to store their personal documents and have a secure backup plan, if the data breach issues occur. It can be sue to this fact that they believe cloud storage services’ providers who are offering the service and working in the market must be enough secure, rather than offering an unsecure service to the market as it may get court by some users if security breach incident happens or at least lose their customers, easily.

6.4 Cloud Forensics’ Challenges

Participants responded on the challenges for cloud storage forensics in Malaysia and the results are shown in Figure 4. As it is shown in the figure, more than one answer was acceptable in this question and the values are in percentage. The results show that the respondents take it very serious, as Malaysia is not a developed country such as Singapore [58]. So, in order to become a developed country, Malaysia not only need to focus on the industrialization, but also the country needs more efforts in information technology industry as it is also a part of the developments, as well [59].

![Cloud Storage Service's Security](image)
lack of jurisdiction when a crime incident happens. Besides that, 86% of participants agree it is very significant that there is a lack of forensic experts in Malaysia and also 75% believe the lack of experiences is very significant issue in Malaysia. It means that if any crimes related to the cloud storage happens in Malaysia, forensics experts will not able to investigate the issue.

The results have shown that the respondents are no sufficiently confident or believe the forensics experts in Malaysia can investigate and overcome any incident, if occurs. A majority of 80% feel lacking in laws and regulations when advisory needed. Thus, this is not a healthy thought for Malaysian who believes the Malaysia enforce department will not able to take any actions against the crime. Besides that, some of the respondents believe the recent cases happening in Malaysia are the reasons causing the society feel not confident for the investigation.

7 CLOUD STORAGE SERVICES DEVELOPMENT in MALAYSIA NEXT 10 YEARS

In the Figure 5, the speculation from 76% of the participants was agreed that the cloud storage services would be more efficient and using by most of the population in Malaysia. This is because the world has improving especially the information technology is growing speedy and Malaysia will have no choice to follow the world’s footstep. However, 24% of the participants are disagree and believe that cloud storage services in Malaysia will not be efficient in next 10 years as Malaysia, and is facing obstructions from many aspects [60]. Furthermore, the authors got some thoughts and comments from the 76% of respondents. They believe the Information Technology will change the culture of Malaysians living style for using any technology products in the future. For example, people nowadays are able to sign any documents using an electronic signature documents rather than get a physical signature documents, like 20 years ago. On the other hand, a group of 24% of respondents believe that the governments’ policies may stop and drag the growing processes or might be an obstruction for Malaysia to achieve the Vision 2020, which has been introduced by the fourth prime minister of Malaysia, Tun Dr. Mahathir Mohamad. In addition, according to H.S. Borji, Malaysia is not considered as a developed country, because the level of industrialization and overall standard of life style are not on par with the most well known developed countries in the world, such as the United States of America, United Kingdom, Singapore, Australia, and Russia. Therefore, Malaysia still have to do more with the country development, and one of the priority
The development process can absolutely be the Information Technology development.

![Cloud Storage Service in Malaysia next 10 years](image)

**Figure 5**: Cloud Storage in Malaysia next 10 years

### 8 CONCLUSIONS

The analysis of results in this study has shown a very low level of awareness for cloud storage services amongst the Malaysians, at the moment. It could be from many aspects of view, culture of Malaysia or government’s policies. Furthermore, the cloud forensics raise significant challenges of cloud storage forensics and those challenges are not ignorable by the related departments such as police, forensic investigation departments, and cloud computing experts. Hence, that is an urgent need in the establishment of cloud storage forensics abilities and performance, which included a set of procedures for conducting an investigation. However, cloud storage services are bringing some new opportunities to the society, as people will change the way they are living and get things done efficiency and faster. Lastly, a preparation for Malaysia to control and supervise the internet must be considered, as so far no serious cloud storage services’ crime has been happened or reported, in Malaysia. This might be the thing that caused the lack of experienced investigator. Thus, the society and the related departments will get panic if it happens. Furthermore, to become a developed country, improving and increase Information Technology is one of the main concerns. This is because, the IT can improve different aspects of developments in a country. For example, the demand of the IT is getting wide and huge as the market shaped by the modern technologies. Consumers are tending to search information about products through IT platforms like Alibaba or other online purchase websites.

### 9 FUTURE RECOMMENDATIONS

This study has shown high satisfaction and responses in most of the items in the questionnaires. Through this research, the authors are able to know the level of awareness for the Malaysians about cloud storage services in this country. Furthermore, even though the level of awareness is very low and it should be a “wake up call” for Malaysians to know that this is not just a trend for Information Technology, but it is also a service that users should know and be aware of its hidden security issues. This study was successful to test and get to know about the awareness of the cloud storage services’ users. The authors believe that this research would help the relevant organizations and government departments to spread awareness through information sharing on cloud storage for users to be prudent on what data they should and what data they should not be uploading to the cloud storage. Besides that, system developers are encouraging to develop more forensics and security tools for the investigators when they really needed for investigations purpose.

### REFERENCES

38. D. Quick and K. Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants", Future


