CHAPTER TWO

LITERATURE REVIEW

2.0. Introduction

Literature review is a very critical and important stage in any research. A good review is important in order to provide evidence that researchers need for their studies (Creswell, 2012). In this research, a systematic literature research is performed on information privacy concerns in cloud computing. The main academic databases are used to use relevant literature such as IEEE, Science Direct, ACM, Springer, Scopus, and the searching engine of Google Scholar. This research uses 'information privacy issues', 'information privacy concern', 'information privacy challenges of cloud computing' as the major keywords for search.

This chapter provides reviews of information privacy. It also gives an overview of e-learning, e-learning in the malaysian higher institution, the information privacy in e-learning of the cloud computing. It also highlights on existing literature of cloud computing information privacy frameworks, theoretical background of information privacy concernsand information privacy issues in cloud computing. At the end of the chapter, the proposed conceptual framework and hypotheses are proposed and explained.

2.1. Privacy

Privacy is an essential human right which is recognized in the majority of international treaties and agreements on human rights. Almost all countries around the world identify the privacy as a basic human right in their constitution, either explicitly or implicitly (Tan, 1999). The importance of the protection of the privacy as an essential human right has been recognized after the disaster and carnages of second World War

period, when large databases of personal data were used to segregate populations, targeted minority groups and make possible genocide, made it clear how it can be dangerous to allow the public to intervene in the private sector. However, the post-war period is seen the appearance of the Universal Declaration of Human Rights (UN 1948).

In the 1970s, the private sector began to use personal information. This increased the risk of personal data being abused and created concerns that there would be a need for regulations to guarantee that individuals' privacy is appropriately protected. Therefore, specific regulations to govern personal data processing were presented at an international and a national level in the 1970s and 1980s (Baumeister, 2006).

Privacy rights or obligations are about the collection, use, disclosure, storage, and destruction of personal data or personally identifiable information (Mather, Kumaraswamy, & Latif, 2009). It is relating to the protection of person autonomy and relationship between a person and the public (including, people, governments, companies, and any other institutions) (Banisar, 2011). Privacy varies between countries and individuals on the basis of past experiences and cultural understandings (Banisar, 2011). It is also constituted by public expectations and legal interpretations. Privacy is a multipart concept with several various directions. Tan (1999) divides privacy into four general facets:

- Information privacy, which is concerned with the control and handling of personal data.
- Bodily privacy, which involves the integrity of an individual's body against invasive procedures.
- Privacy of communications, which covers individuals' interests in communicating among themselves using various forms of communications.
- Territorial privacy, which involves setting limits or boundaries on intrusion into a specific space or area.

With the growing ability and implementation of technology, the digital world carries additional complexity in many ways, such as information privacy. Recently, inforamtion privacy is being more challenged (Hustinx, 2010). The new technologies entail a huge increase in the collection, share and exchange personal data often without individuals being aware of it; much less controlling it. Sensitive personal information is now gathered and used consistently (Banisar, 2011). Previously, the only way to steal is to break into the property. Nowadays, with small tools, ones can steal information without any effort, and strangers can steal information from outside without reaching the property.

The modern and cheap techniques for gathering, storage, analysis and use of information have increased and impinge upon our lives in ways innumerable and varied (Humphreys, 2011). By technology, it is possible to track an individual activity, locations, habits and work (Hustinx, 2010). Moreover, the widespread use of social networks, a large personal information public records are being available and disclosed over the Internet around the world. In response to this situation, some countries have implemented comprehensive laws to grant individuals some control for collection and use of data by public and private sector (Banisar, 2011). In brief, although technology has made life easier, it has largely traded inforamtion privacy and put our information privacy at risk.

2.1.1. Information Privacy

Information privacy is defined by Westin (1968) as an individual's right to control, edit, manage, and delete information about them [selves] and decide when, how, and to what extent information is communicated to others. With an unprecedented amount of personally identifying information, information privacy is considered as critical issues which can influence ethical, legal, social, and politics. The main matter in information privacy is the control of information (Katzan Jr, 2011). Some studies have viewed various perceptions of information privacy (moral, legal right and the ability to control personal information) (Bélanger & Crossler, 2011; Clarke, 1999) while, users see that only users should have the ability to release their information. Some organizations also suppose that the organization that collect, create maintain and process the

information have rights to control of it (Goodhue & Straub, 1991). In addition, personalized technologies offer powerful tools for enhancing the user' experiences and it requires to collect and mining of user information such as what users like to read, what users like to buy, how much time s/he spends. However, if any company has sold users' information to another company, it will be effectively violation user's information privacy.

In summary, the immense growth and development of information technology give rise to the importance of protecting the individual' information privacy. And rather than accepting a complete loss of information privacy, as an inevitable part of technology, is essential to look for ways to preserve the information privacy, and to gain the benefits of technology without being forced to give away people's information privacy.

2.2. E- Learning

The rapid development and use of information and communication technologies (ICTs) have a positive impact on the educational process. This fundamental effect has been illustrated in the form of e-learning. The use of ICTs for education has improved and has provided motive for e-learning practice to grow dramatically putting the educational institutions under pressure to involve new technologies in their learning process (Kahiigi, Ekenberg, Hanson, Danielson, & Tusubira, 2008). Most of the traditional learning methods are becoming inadequate to the needs of social evolution and not being able to catch up the rapid development of learning in time. E-learning is a broad term that includes the use of a computer to support learning in a broad diversity of learning approaches and ICT applications for exchanging information and acquiring knowledge. The ICT applications include radio, television, discs, video conference, mobile technology, web-based technologies, discussion forums, and other methods of communication (Sahu & Singhal, 2002). In addition, the social technology has changed

not only the learning process but also beliefs, preference, senses, opinions, and culture of the people, made learning exciting, active, competitive, influential and comprehensive.

This innovative approach to learning assures to transfer the classroom experience in various ways: by augmenting traditional textbook with electronic material; classroom with various multimedia technologies (Audio, Visual Technology, Graphics, 3D, and Digital Image), and by widening learner discussions beyond the classroom walls via a wide variety of new interactions platforms supporting inter-classroom cooperation. On the other hand, it is not possible to fully replace face to face learning to virtual education with excluding several institutions which may work entirely on the Internet (Sahu & Singhal, 2002). E-learning has many advantages such as flexibility, diversity, measurement, personalization. It becomes one on the most important methods for learning in this century (Laisheng & Zhengxia, 2011).

Most major universities of the world offer e-learning system to support the learning process. E-learning is one of the best responses to the increasing need for education. The E-learning has a positive impact not only for students but also for instructors and educational institutions. There are wide varieties of tools that have been developed and used to support learning, such as learning management system (LMS), Education Learning Management Systems (ELMS), learning content management system (LCMS) and Virtual Classrooms. These tools have some common features whether it is open source or commercial. These tools provide the learning material. This material is divided into modules and lessons with various types of users based on the user role (learner, instructor, and manager).

On the other hand, students in the 21st century have distinctive and unlimited learning needs that no longer can be fulfilled with traditional educating and learning systems. Thus, e-learning systems require much more hardware and software resources and there are many educational institutions that cannot afford such investments. Therefore, the cloud computing technology can be a useful solution to reduce most of these issues.

2.2.1. E-Learning in Malaysia Higher Institution

Over the past few decades, the Malaysian higher education system has more intensity and quality. The Ministry of Higher Education (MOHE) is responsible for the operation of higher education institutions (HEIs). The Malaysian higher education system has made a significant increase in student engagement, raised in global recognition on many fields such as research publications, patents, and institutional quality, as well as becoming one of the main targets for international students. Malaysia is one of the preferred destination for higher education students around the world (World-Education-Network, 2016). Currently, Malaysia ranked 11th worldwide by UNESCO for its appeal to students. The numbers of international students at higher institutions have increased significantly in the last ten years (StudyMalaysia, 2015). In 2011, HEIs in Malaysia has housed about 93,000 international students from more than 100 countries, and with a target to increase up to 200,000 students by 2020 (MOHE, 2015). These successes are evidence of the paradigm shift and innovation of the Malaysian academic community.

Most of the educational institutions in Malaysia have implemented e-learning in order to meet the needs of the population growing and the needs to compete globally. Based on 26 higher education institutions (HEIs), which have been surveyed by Embi (2011), 42.3% of HEIs offered more than 50% of their courses online. A total of 15.4% of HEIs offer 0–10% courses online. While 11.5% of HEIs offer 11–20% courses online, 11.5% of HEIs offer 21–30% courses online, 11.5% of HEIs offer 31–40% courses online, and 7.7% of HEIs offer 41–50% courses online as shown in Figure 2.1.

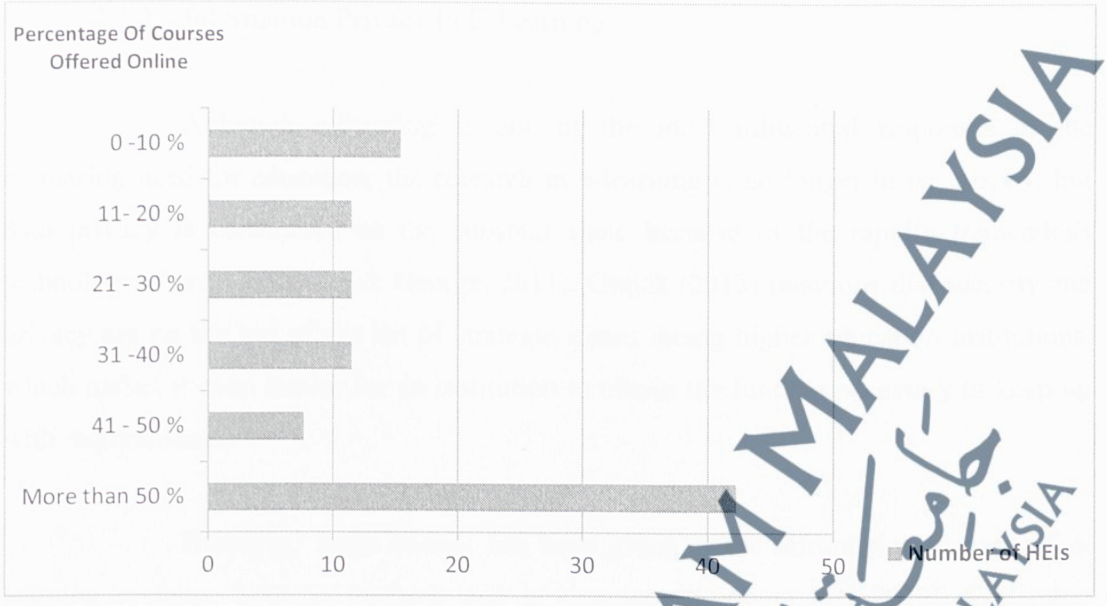


FIGURE 2.1: Percentage of Courses Offered Online By Education Institutions in Malaysia

Like other educational institutions around the world, universities in Malaysia as will face the challenge in guaranteed quality as well as efficient teaching and learning the process. The public universities have to work with a limited budget given by the government. Furthermore, public universities have a large number of students and there are some issues such as software constant licensing, infrastructure, teaching materials, training of lecturers and the renovation is very slow (Salleh, 2008).

It is important for universities, especially in Malaysia, to implement new methods and technologies that will better prepare and equip students for learning needs (Razak, 2009). Adopting cloud computing technology gives all the needs of educational institutions to improve teaching and learning methodologies in Malaysian universities (Kassim, Salleh, & Zainal, 2015).

2.2.2. Information Privacy In E-Learning

Although e-learning is one of the most influential responses to the increasing need for education, the research in e-learning is no longer in its infancy, but data privacy is considered as the constant issue because of the rapidly tremendous technological progress (May & George, 2011). Grajek (2012) mentions that security and privacy are on the top of the list of strategic issues facing higher education institutions, which makes it even harder for an institution to obtain the funding necessary to keep up with requirements.

However, little interest has been given to the information privacy of e-learning systems, both in research and in practice (Kambourakis, 2013). E-learning information privacy has an exclusive challenge as these systems are used and managed online by thousands of users and networks. On the other hand, the majority of e-learning researchers has focused on course development and delivery, with little or no consideration to information privacy as essential elements (Ball, Ramim, & Levy, 2015; Kambourakis, 2013).

In e-learning environment, users have many information privacy concerns for what will happen to their information being gathered by the system. Users need to be independent to have a sense of autonomy in asserting their beliefs, ideas, and values (Grajek, 2012). On the other hand, in order to provide users with personalized e-learning service, a huge number of personal education information can accumulate over time which is collected by e-learning system. It includes not only the users' information such as name, age, gender, race, language, address, telephone number, date and place of birth, job title, physical mailing address, e-mail address, financial information such as credit card information, but also includes the users' educational information such as knowledge structure, knowledge level, and knowledge scope, learner's intelligence level, study content, learning material, rank, weak points, and learning rule. In addition, all the activities of the users could be stored in e-learning system such as the history of learning activities, the contributions to electronic discussions/forums. This data can provide deep

insight into sensitive information such as users' activities, interests, thinking, beliefs and even the political views (Weippl & Tjoa, 2005).

There are several reasons why e-learning users might want to keep their data private. For instance, students may need to protect themselves from a biased lecturer. The bias of the lecturer may come from prejudice or stereotype, based on a past experience with students, or even from individual reasons (Aïmeur, Hage, & Onana, 2012). Also, some e-learning system contains external links to other websites involving the learning content providers, like libraries, academic websites. However, e-learning system has no control over the data and is not responsible for, the content of, or information gathered by those other websites. If users click through these links, some personal information will be transmitted in the form of leading to the third party. Then unlimited contact via e-mail, phone or direct mail will be brought (Grajek, 2012).

There are many information privacy concerns about the personal information that are gathered by cookies or other techniques which are used by an e-learning system to exchange with other e-learning system partners or any advertising companies. If a cookie can get this information, then it might be shared with commercial use especially, if the location of the students is stored as well (ICL, 2014). Furthermore, the creation of learning material always needs a substantial amount of human expertise and cannot be automated to a significant degree. Therefore, learning material will constantly represent a high quantity of expertise and effort. The copyright holders of learning material have a strong interest in protecting their learning material from illegal use and sharing (Kim, 2013). Another information privacy concern is the storage of discussion threads and personal annotations in an e-learning system which constitutes a risk to the information privacy of teachers and students. Even if the course is deleted from the server, there may still be existing copies of the content such as backups. Students store their content on different servers that are not under the school's control. The servers are usually located in other countries, which mean that laws and regulation will be different. Table 2.1 summarizes the type of information in e-learning system should be kept private.

TABLE 2.1: Type of information need to be protected

Sensitivity Level	Privacy Level	Type of Information
Low sensitive information	These personal data may be exchanged without any security or privacy protection.	Name, age, gender, race, language, address, telephone number, date and place of birth, job title, physical mailing address, e-mail address
Medium sensitive information	These personal data may only be exchanged to particular parties	knowledge level, and knowledge scope, learner's intelligence level, study content, learning material and learning rule
High sensitive information	These personal data may never be exchanged to other parties.	Knowledge structure, biometric information, Financial information, History of learning activities, the contributions to electronic discussions/forums

Source: (Pearson, 2009)

It is obvious from the literature that there will be a growing need for high levels of information privacy in e-learning system as users have many information privacy concerns for what will happen for their information being collected. The information privacy issues and concerns involved in the e-learning system will minimize the value perception of these systems. Providing recommended procedures, frameworks, assessment tools and policies to ensure the information privacy of users' information is necessary and key factor in minimizing the users' information privacy concerns. Thus, the next innovations of e-learning system should consider the new challenges of rapid technology growth to meet these needs.

2.3. Cloud Computing

Cloud computing is an emerging new computing model for delivering computing services. It represents a shift away from computing as a product that is purchased, to computing as a service (Lamba & Singh, 2011). Cloud Computing provides computing resources with a high level of availability, scalability, elasticity, and free of maintenance (Lu, Xu, Huang, Chen, & Chen, 2011). The computer resources of the cloud computing are increased when the users need and decrease when they need less. The cloud computing is seen as the significant shift of information industry and will make more

effect on the growth of information technology for the society (Liu, 2012). Cloud computing provides an additional flexible way to use computation and storage resources to meet business needs on demand. Cloud computing users can access to these resources via the internet often by using a thin client like a web browser. Cloud offers services that can be grouped into the following categories.

2.3.1. Service Deployment Models

There are three main commonly used categories of cloud deployment models: Private Cloud, Public Cloud, and Hybrid Cloud. While, the community cloud model is less-commonly used. Following is the brief description of each category of cloud computing:

Private cloud is cloud infrastructure runs exclusively for a single organization. Private Cloud could be owned, controlled, and operated internally, externally by a third party or internally and external at the same time. The infrastructure can be either on premises or off premises. This deployment model gives the organization more control of the infrastructure and data. This main feature avoids many security and privacy issues but it is more expensive than other model (Mell & Grance, 2011).

Public cloud is the most common model of cloud computing. It is offered over the Internet and is owned and operated by a cloud provider. Constructed using pooled shared physical resources, and accessible over the internet. The main feature of the public cloud is cost saving because the cloud infrastructure is dedicated for use by the general public (Mell & Grance, 2011).

Community cloud in community cloud, the cloud infrastructure is dedicated for use by two or more organizations with similar goals and objectives. It could also be at a service providers premises or some part of the infrastructure. It also could be in one or more of the organizations while the remaining part could be at the service providers' premises (Mell & Grance, 2011).

Hybrid cloud or enterprise cloud consists of two or more distinct cloud infrastructures (private, community, or public). A part of the cloud is private and only accessible internally and the other part is public and can be accessed externally (Mell & Grance, 2011).

The Public cloud computing can help in reducing educational institutions' IT complexity and costs by using SaaS to replace the software installation on campus computers with applications delivered via the Internet (Sasikala & Prema, 2011). Public clouds provide access to an almost infinite amount of infrastructure resources without any upfront investment required, and the ability to use cutting-edge technology available from public cloud provider (Butler, 2016). Students, lecturers, administrative staff members and other cloud users in the institution can access educational tools or files saved in the public cloud from almost any internet-capable device (Meske, Stieglitz, Vogl, Rudolph, & Öksüz, 2014). Moreover, students can have access to course content, video tutorials, educational e-books, online exams, and podcasts, workshop / conference videos. lecturers/instructors are also able to upload course content, video tutorials and other educational materials (Olokunde & Misra, 2015).

2.3.2. Cloud Service Models

Cloud computing services models represent how services are made available to users. These services models include a combination of three models which are parallel to the traditional computing environment layers (Mell & Grance, 2011). The Cloud computing services models are a Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as Service (IaaS).

Software as a Service (SaaS) is applications distribution model in which applications are running in a cloud environment. These applications are made accessible to clients from different user devices by web browser so they can access these applications anywhere anytime, retrieve, and save their work (Mell & Grance, 2011).

Platform as a Service (PaaS) is the middle level of clouds service. PaaS is an expansion of Software as a Service. The clients can get all tools that s/he needs to build applications, such as programming software or database software. It can be used for various stages of software development, testing, and deployment. The clients have the control over their applications without a need to manage the server, storage, network or operating system (Ghazizadeh, 2012).

Infrastructure as a Service (IaaS) is the lowest level of cloud computing which contains hardware, as well as basic operating systems and virtualization of hardware resources. It is to ensure the stability and reliability. The clients are provided with the capability to processing, storage, networks and any software. The infrastructure management and maintenance are the responsibility of the supplier (Mell & Grance, 2011).

Among the different service models, SaaS is the most commonly used model in e-learning system of educational insitioation (Akande & Van Belle, 2014). It is made up of systems that can receive, process, and deliver software and applications over a network. Such as, email systems, learning management systems (LMS), customer relationship management (CRM) systems and enterprise resource planning (ERP) systems (Rezaei, Karimi, & Hosseini, 2016; Tashkandi & Al-Jabri, 2015). SaaS can provide users with software and applications for writing documents, analyzing and collecting data, formatting and organizing references, communication (Shakeabubakor, Sundararajan, & Hamdan, 2015). Google docs, dropbox and office 365 are popular SaaS offerings used by students and lectutres in e-learning system of education education insitioation (Erturk & Iles, 2015).

Several educational insitioations have adopted SaaS e-learning system because of its promises such as cost reduction, scalability, flexibility, pay per use model, accessibility. Software and applications available through SaaS are being used by students and lectutres in education insitioations mainly for collaboration, content delivery, communication and accessing learning materials (Erturk & Iles, 2015). The economic

advantages, speed, agility, flexibility as well as infinite elasticity of SaaS which leads to improved e-learning services (Alsaeed & Saleh, 2015).

However, a number of challenges have been identified which might have a negative impact on the predicted growth of the SaaS adoption. Among these challenges, privacy issues have been repetitively raised as threats to SaaS adoption (Akande & Van Belle, 2014; Alharthi, Yahya, Walters, & Wills, 2015). Privacy has emerged as the key inhibitor of SaaS adoption (Gashami, Chang, Rho, & Park, 2014). Thus, this research focuseson informatio privacy issues of using SaaS in public cloud in e-learning sytem.

2.3.3. Characteristics of Cloud Computing

The Cloud computing presents many significant features that is different from traditional computing service. In general, there are four essential characteristics of cloud computing which are:

On-demand self-service Computing cloud resource such processing power, network storage, virtual machines as be gained and utilized at any time without requiring any human interaction (Mell & Grance, 2011).

Broad network access The cloud resources could be gotten over a network by a variety of platforms such as laptops, tablets or smartphone (Mell & Grance, 2011; Puthal, Sahoo, Mishra, & Swain, 2015).

Rapid Elasticity Computing resources in cloud computing such as CPU, memory and storage are able to scale out and quickly as needed based on demand. The cloud appears to be infinite to the users, and can be purchased in any quantity at any time (Mell & Grance, 2011).

Measured Service Cloud computing has the potential to automatically control, monitor and optimize the resource use to all types of service such as storage,

processing, bandwidth, and active user accounts while each cloud provides users has a different level of abstraction (Sasikala, 2013).

2.3.4. Cloud based Massive Online Open Courses

Massive Online Open Courses (MOOCs) represent a recent trend in online education, which many universities offering quality courses through Cloud platforms. Cloud service providers offer many free platforms and software to set up online MOOCs for constructing a learning space such as Coursera, edX, Udemy, and Udacity. By hosting learning resources in the cloud, students and teachers are able to explore learning resources more quickly and easily. MOOCs offer to students an opportunity to learn from the best educators at some of the world's top universities with no cost (Gaebel, 2013), with rapid grow in technology make easily of many MOOCs reached thousands of participants from all over the world in one course. MOOCs are to offer a new option to a massive number of people to attend online courses for free wherever they are (Gaebel, 2013).

However, the assessment is an essential issue of MOOC. MOOCs do not offer formal accreditation of institutions, which show the different value of learning outcome between MOOCs and academic institutions courses (Sandeen, 2013). MOOCs providers are given a non-credit certificate such as participation, completion or attendance certificate (Yousef, Chatti, Schroeder, & Wosnitza, 2014).

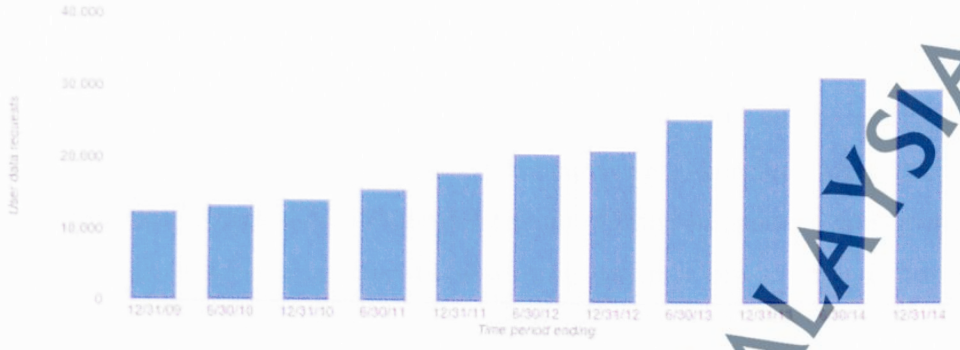
Massive open online courses in Malaysia are a recent development. The first MOOC in Malaysia is offered by the School of Engineering at Taylor's University in March 2013. Malaysia is the first country in the world implement the MOOCs initiative for public universities (Open-Learning, 2016). In 2016, there are twenty public universities that have embarked on a MOOCs initiative. In addition, Malaysia plane to be the first country in the world to develop a national policy on credit recognition for the (MOOCs). The public universities offered over 63 courses and more than 192000 students are involving (Open-Learning, 2016).

2.3.5. Information Privacy of Cloud Computing

There is a gap between CSPs and cloud users regarding information privacy and transparency in the cloud. CSPs response to the information privacy suspicions: *"Clouds are more secure than whatever you're using now"* (Kshetri, 2013: P 372). On the other hand, many studies and surveys show the information privacy is the main reason for slowing to adopt the cloud computing. People are often concerned y and uncertain about hidden costs related to information privacy breaches or lawsuits related to the violation of data via cloud computing (Goodburn & Hill, 2010). People are still cautious in using cloud computing to upload their high-value or sensitive data (Goodburn & Hill, 2010). In the past few years, there are many information privacy breaches happened. The following are some examples of information privacy breaches in Google cloud.

According to Svantesson and Clarke (2010), Google Docs' Information privacy Policy shows that users can gain only very limited knowledge of how their personal information could be used and where the data is stored by Google. Moreover, Google makes it clear that they may combine the information that consumers submit under their accounts with information from other Google services or third parties (Google, 2015).

In 2009, Security vulnerability has been discovered in Google Docs, which revealed documents for users belonging to other users. The vulnerability was fixed during hours, but it showed that users' information could be declared to others (Svantesson & Clarke, 2010). Furthermore, Google declares that the information that is already available elsewhere on the Internet or in public records is not to be regarded as private or confidential. Google also has the right to direct advertising to the users. In addition, based on Google Transparency Report, in the first half of 2014 and the second half of 2014, Google received 31698 and 30140 requests for disclosure user data, 9,981 requests are from the United States. Google provided user data to the US government in 78% of the requests (Google, 2015). Figure 2.2 shows the user data requests by reporting period.



Source: (Google, 2015)

FIGURE 2.2: User Data Requests by Reporting Period

In 2016, Yahoo Company, that offers cloud service, has confirmed that at least 500 million user account credentials are breached in late 2014. The stolen data includes names, email addresses, telephone numbers, birthdays, hashed passwords, and some encrypted or unencrypted security questions and answers (Leswing, 2016). However, such breach raises many information privacy issues because the stolen information from Yahoo includes unencrypted questions and answers to security questions. This could be used to reset account passwords. In this case, the users' information would be out of control and the Yahoo would not be able to provide the users access to their account. Moreover, Yahoo has taken two years to disclose this breach to the public which raises the information privacy breaches notification issue. These issues are also involved in how Yahoo monitors the service. Furthermore, with significant information held offshore by companies like Yahoo, the information privacy concerns of a cross-border information flows, regulation and compliance that govern the data should also be taken into consideration.

2.3.6. Information Privacy Issues in Cloud Computing

Pearson (2009) states that one of the key features of the public cloud computing is an infrastructure shared between organizations. Therefore, there are issues related to stored and processed data somewhere remotely, and because there is growth in the use of virtualization and sharing of platforms between organizations. Protected personal and sensitive information that is stored in the public cloud is essential to guarantee the information privacy of one user's data from another (Foster, Zhao, Raicu, & Lu, 2008). Without considering information privacy issues, the adoption of cloud computing can be discarded by large spectra of organization and users (Ghorbel, Ghorbel, & Jmaiel, 2017). In consequence, the users have lost their control over the data and depend on the cloud service provider. Such change leads to a number of privacy concerns to be raised. The most common information privacy issues of cloud computing in the literature are as follows:

2.3.6.1. Access

The main concern is whether the organization is able to provide users who have only the right to access data and modify it if inaccurate (Mather et al., 2009). Cloud users must be able to obtain access to their data, to perceive what is being held about them, and to check its accuracy (Pearson, 2009) . If user's data is locked-in and cloud service providers fail to provide access, this service disruption could pose potential damage to the users. In addition, storing data that reside outside the organization's especially in public cloud premises poses the potential risk of unauthorized access (Mouratidis, Islam, Kalloniatis, & Gritzalis, 2013). There is also a threat of steal or misuse of customers' data by co-hosted customers, rogue employees of the service providers, subcontracted services, foreign governments, or attackers breaking into the networks (Mowbray & Pearson, 2012). Moreover, the users have a right to be known with what information is being held, and they have a right to make a request to stop processing in certain cases (Mather et al., 2009). The users should be able to find out how and by whom his data are handled (Ghorbel et al., 2017).

2.3.6.2. Compliance

Compliance indicates the list of applicable laws, regulations, standards and contractual commitments that govern cloud computing data (Singh & Goel, 2015). Conflicting issues may arise because the distributed data in the cloud may have different legal location laws that apply at the same time (Gellman, 2012). Legal compliance is a significant challenge for public cloud because a large number of information security and data privacy laws exist, depending on the country and location (Mouratidis et al., 2013). Mowbray, Pearson, and Shen (2012) also highlight that several countries rules may limit processing and storing of personal or sensitive information on cloud computing that does not adhere to the regulatory requirements. Although data security laws and regulations are not similar in various countries around the world, there is no existing information privacy standard or comprehensive legal framework which can organize and manage the rights and boundary of CSPs and cloud service customers (Mouratidis et al., 2013). Both CSPs and cloud service users have to deal with existing regulatory requirements and service level agreements.

However, CSPs may be compelled to disclose users` data to the government request regarding national security or to local regulatory. The law is obligatory where the data is obtained or where data is transferred (Zhou, Zhang, Xie, Qian, & Zhou, 2010). There is possibility that user's data may be transferred across international boundaries without having the adequate controls to guarantee compliance and protection of the information. Therefore, it is necessary to identify compliance issues such as legal rights and alignment of SLA with legal obligations, protection, and enforcement requirements before deploying a cloud computing solution (Mouratidis et al., 2013). In general, the legal situation is subject to change: legislation has not yet been updated to address privacy challenges in the cloud (Mowbray & Pearson, 2012).

2.3.6.3. Storage

The physical location of the cloud server brings up additional questions. One of the public cloud computing features is a dynamic environment. Services can potentially be aggregated and changed dynamically by users, and service providers can change the provisioning of services. In such scenarios, personal and sensitive data may move around within an organization and/or across organizational boundaries (Pearson, 2009). Information privacy laws in different countries restrict the ability of organizations to transfer some types of data to other countries. Conflicting issues may also arise as many locations of stored data have different regulations that are valid at the same time. In addition, storing data on the different location may lead to the unauthorized access (Singh & Goel, 2015). Information privacy risk can be increased because of foreign country surveillance as the data may be transferred to another data center without the knowledge of the organization, which has led to the possible violation of domestic law of the country where the data is stored (Pearson & Benameur, 2010).

2.3.6.4. Retention

This retention is associated with time for which user's data is retained on the cloud. This simply means that for how much time a user can have access to the cloud (Singh & Goel, 2015). The retention and ownership of the data on the cloud also become more and more questionable. It is essential that organizations should be aware of how long the retention period of the data on the cloud is; the retention policy that governs the data, the ownership of the data (organization or the CSP) and how to impose the retention policy (Mather et al., 2009). These issues may be arising in some cases, for instance, if CSP stops the services due to any reason or the CSP may decide to mortgage the organization data due to overdue of payment or the service could be suspended for non-payment.

2.3.6.5. Destruction

Destruction is the process of deleting of user's data at the end of the retention period and to ensure that the user's data is destroyed and is not available to another cloud user (Singh & Goel, 2015). However, it is impossible to guarantee the complete deletion of all copies of data (Mowbray & Pearson, 2012). The organization could only be unable to access the data, but the data is actually not deleted. The organization should take into account this issue in regulation and make CSPs responsible for any damage. The organization also should enforce the CSP to not keep their data longer than necessary to avoid any potential information privacy breaches (Mather et al., 2009).

2.3.6.6. Audit and Monitoring

There are several concerns around audit and monitoring in the cloud, these issues involve how the organizations can monitor the cloud provider, and how to provide necessary controls and procedures to assure the users their information privacy requirements are met (Singh & Goel, 2015). However, audit and monitoring have great value as they enhance a sense of trust of organizations about the CSP effort in ensuring the information privacy. Both, providers and users need to comply with existing regulatory requirements and service level agreements (SLAs). SLA should be completed as well as well structured, taking into consideration the right to audit such as quality of service attributes should monitor continuously and enforced by SLA (Mouratidis et al., 2013). While the mentoring should not be intrusive and must be limited to what the cloud provider reasonable needs in order to run their facility, the CSP must be transparent about the information privacy breaches; governance policy and activity report (Zhou et al., 2010).

2.3.6.7. Information privacy Breaches

In the case of any information privacy breaches occur, CSP should be responsible for managing these breaches and should provide the organizations with direct notice of any information privacy breaches so that the organization can handle the situation as effective as possible (Mather et al., 2009). The organization and CSP should also make clear how the breach can be determined and the steps of notification process of breaches (Singh & Goel, 2015). Providers must initiate or offer help in the breach investigation and prosecution. Like security, privacy is an important issue in cloud computing in terms of both legal compliance and trust (Mouratidis et al., 2013). Table 2.2 lists the most common information privacy issues of cloud computing found in the literature.

TABLE 2.2: Information Privacy Issues of Cloud Computing

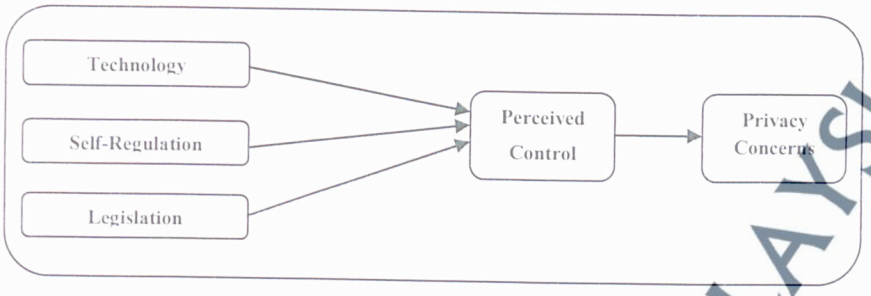
Information Privacy Issues	Literature Support
Access	(Ghorbel et al., 2017; Mather et al., 2009; Mouratidis et al., 2013; Mowbray & Pearson, 2012; Pearson, 2009)
Compliance	(Gellman, 2012; Mouratidis et al., 2013; Mowbray & Pearson, 2012; Singh & Goel, 2015; Zhou et al., 2010)
Storage	(Mather et al., 2009; Pearson, 2009; Pearson & Benameur, 2010; Singh & Goel, 2015).
Retention	(Mather et al., 2009; Singh & Goel, 2015)
Destruction	(Mather et al., 2009; Mowbray & Pearson, 2012; Singh & Goel, 2015).
Audit and Monitoring	(Singh & Goel, 2015; Zhou et al., 2010).
Information privacy Breaches	(Mather et al., 2009; Mouratidis et al., 2013; Singh & Goel, 2015).

2.4. The Existing Information Privacy Frameworks of Cloud Computing

Since the beginning of cloud computing, data information privacy concerns have been recognized as one of the most important topics. Hence, there are various frameworks and models proposed for ensuring the information privacy in cloud computing. The next section gives an overview of frameworks that are relevant to cloud computing information privacy.

The study of Xu (2007) focuses on three leading mechanisms that can alleviate information privacy concerns in the location-based services (LBS) context. This study draws on the control agency and self-construal theories to propose a framework linking three mechanisms (privacy-enhancing technology, industry self-regulation, and government legislation) to information privacy concerns through the mediating effects of perceived control as illustrated in Figure 2.3.

This study operationalized information privacy concerns as a reflective construct encompassing four areas of consumers' concerns about information privacy practices: the collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. Xu (2007) adapts constructs from measurement scales used in prior studies to fit the LBS context. The researcher selects one item from each of the four perspectives of the information privacy concern instrument developed by (Smith, Milberg, & Burke, 1996). The data is obtained from 141 mobile phone users. Result shows that all the three mechanisms are effective in increasing perceived control, which in turn mitigates information privacy concerns. In addition, people who value independent-self prefer personal control through technology-based mechanisms; whereas people who value interdependent-self prefer proxy control through industry self-regulation and government legislation.

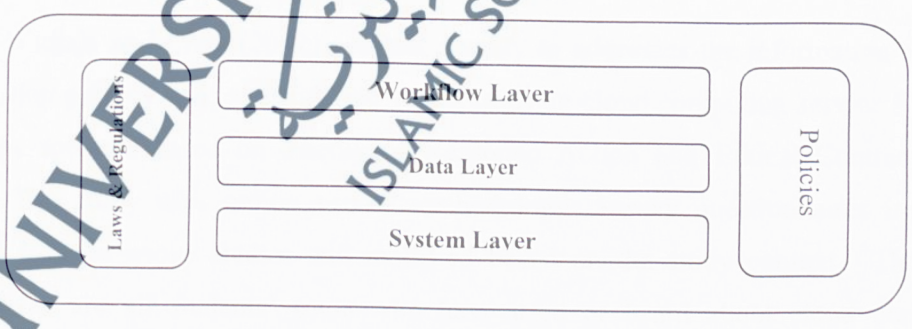


Source: Concerns (Xu, 2007)

FIGURE 2.3: The Effects of Self-Construal and Perceived Control on Privacy

Chen and Yoon (2010) present a framework for secure cloud computing through IT auditing. Their framework is based on checklists by following data flow and its lifecycle. The checklist focuses on the data location awareness, data ownership awareness, data lock-in, data processing isolation, and data protection plan and best practice.

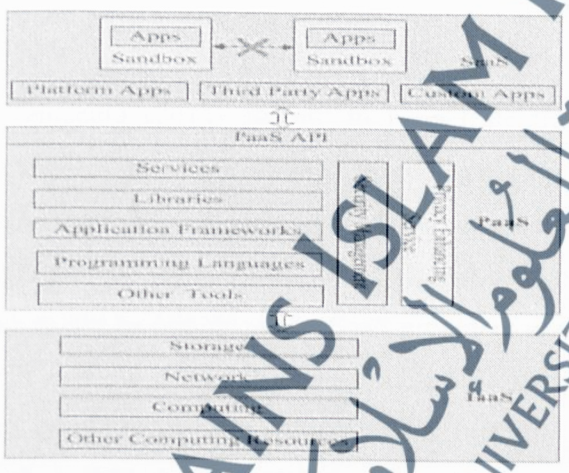
Ko et al. (2011) present a trusted cloud through using detective controls with Trust Cloud framework, which contains three layers (System Layer, Data Layer, Workflow Layer) of accountability as illustrated in Figure 2.4. The framework focuses on achieving a trusted cloud rather than the security of user's privacy. However, it could not address the issue on violations of users' privacy data by provider, even though the cloud is trusted.



Source: (Ko et al., 2011)

FIGURE 2.4: Abstraction Layers of Accountability in Cloud Computing

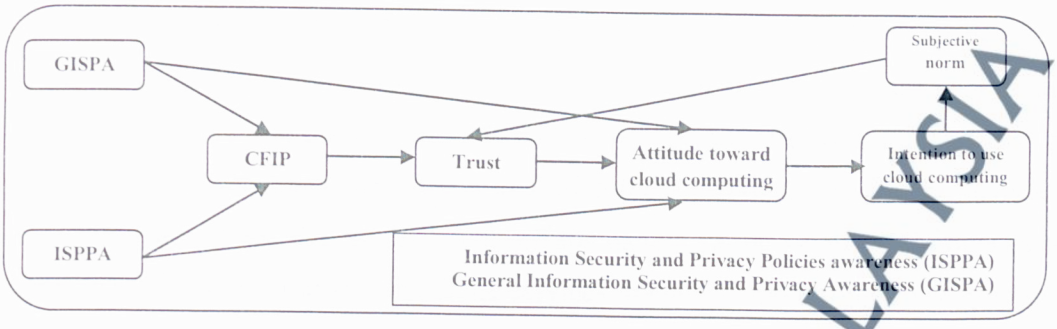
Zhao, Li, Li, Zhang, and Tang (2012) propose information privacy enhancing framework on PaaS for discovering the information privacy violating behavior and protecting user's information instantly by enforcing related protection actions as shown in Figure 2.5. The proposed framework allows customized security policies and behavior analysis models, enabling users to impose application oriented information privacy monitoring mechanisms. However, this framework still has its flaws. So far, it only provides a scheme for the PaaS to install the framework. Without addressing the existing flaws and the framework does not yet implement in practice.



Source: (Zhao et al., 2012)

FIGURE 2.5: Privacy Enhancing Framework on PaaS

Widjaja and Chen (2012) conduct a study to addresses the information security, information privacy concern, and trust issues in using cloud computing service from end users' perspective based on Theory of Reasoned Action and Ethical Contract based theory. The study uses online survey methodology. Survey questionnaires items are adapted from previous studies and modified based on the study context. The target respondents are all students' users who have used or heard about cloud computing services. There are 201 total respondents answering the survey. The result confirms all paths that are shown in Figure 2.6.



Source: (Widjaja & Chen, 2012)

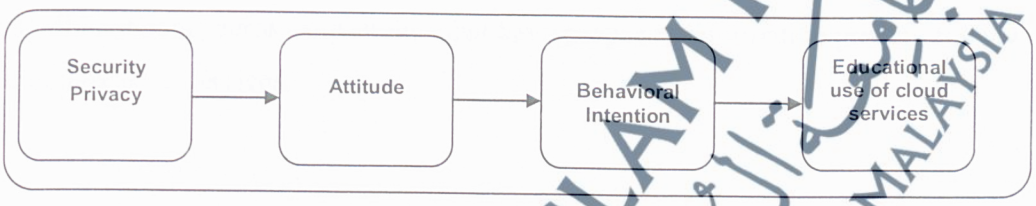
FIGURE 2.6: The Basic Model of Information Security and Privacy in Using Cloud Computing Service

Burda and Teuteberg (2014) attempt to investigate the factors that influence individual users' intentions to use SaaS and provide an empirically-verified privacy calculus model that is specific and tailored to the unique environment of SaaS. The expected results might provide specific benefits that might be maximized and the adverse privacy concerns that might be minimized by SaaS providers to encourage individuals to use their services. They plan to collect around 300 observations from active SaaS users in South Korea through online survey method to test our structural model and hypotheses. The proposed research model is in Figure 2.7.

Source: (Burda & Teuteberg, 2014)

FIGURE 2.7: The proposed privacy calculus model

Arpaci, Kilicer, and Bardakci (2015) have proposed a research model based on Theory of Planned Behavior (TPB) (Ajzen, 1991) which posits that student attitudes predicted by security and privacy perceptions and behavioral intentions are predicted by attitudes towards using cloud services. A total of 200 usable questionnaires are analyzed. The results also indicate that security and privacy have a strong significant influence on the students' attitudes towards using cloud services in educational settings. The proposed research model of Arpaci et al. (2015) is illustrated in Figure 2.8. However, the study was delimited from the examination of the subjects who never use such services.



Source: (Arpaci et al., 2015)

FIGURE 2.8: The Effects of Security and Privacy Concerns on Educational Use of Cloud Services

Despite the above, researchers focus on information privacy of cloud computing, the information privacy issues in cloud computing in literature have been addressed generally. Most of the researches have listed these issues and do not test how these issues could have an effect on the information privacy concerns such as (Mouratidis et al., 2013; Popović, 2010; Widjaja & Chen, 2012; Zhou et al., 2010) . There is limited research that investigates why the users concern about the information privacy in the cloud. Most of the previous frameworks have addressed or tested the information privacy concerns factor in general but they do not investigate the reason. For this concern, they also do not identify the issues that may affect the information privacy concerns such as (Arpaci et al., 2015; Ko et al., 2011; Widjaja & Chen, 2012; Xu, 2007; Zhao et al., 2012) .

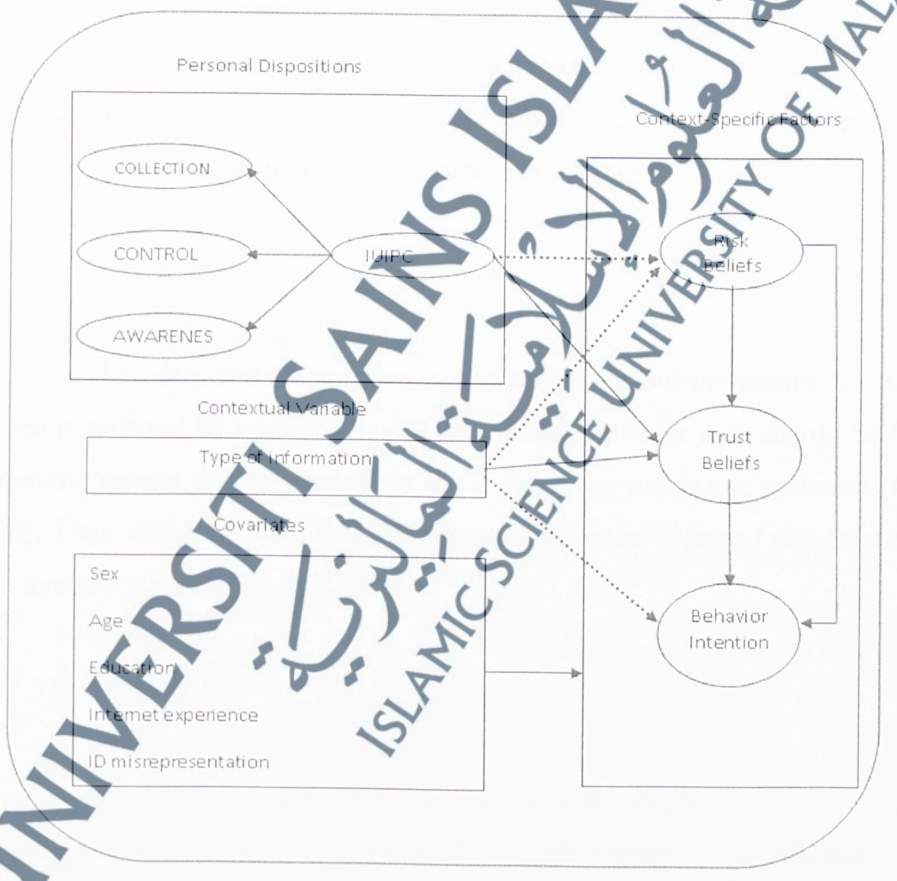
On the other hand, the other studies focus on evaluating the security issue more than the privacy issue. To the best of our knowledge, the only study by Burda and Teuteberg

(2014) have tested the privacy issues in cloud computing which adopts the CFIP framework that has four dimensions (collection of personal information, unauthorized secondary use of personal information, errors). However, this study has not covered all the privacy issues of cloud computing such as (compliance, storage, retention, destruction, audit and monitoring, and information privacy breaches notification). Therefore, the present study sets out to take an initial step in filling this gap by identifying the factors that effect on information privacy of cloud based e-learning users. To the best of our knowledge, this is the first study to investigate the factors that influence n information privacy of cloud based e-learning users. Unfortunately, the researcher in this study did not come across any studies that have proposed information privacy framework in cloud based e- services.

2.5. Theoretical Background of Information Privacy Concerns

The research of information privacy is becoming more and more important among information system researchers. Various approaches to clarify the diversities of information privacy concern levels or to explore the influence of information privacy concerns on several factors have been proposed in the literature across many disciplines or domains (Bélanger & Crossler, 2011; Dinev & Hart, 2006). The concept of "information privacy concerns" has become the essential construct within information system researched and has carried out as an alternative to using the concept of information privacy (Xu, Dinev, Smith, & Hart, 2011). The information privacy concerns have been defined by Malhotra, Kim, and Agarwal (2004: P 337) as the "*individual's subjective views of fairness within the context of information privacy*". Milberg, Smith, and Burke (2000) suggest that information privacy concerns effect on individuals' attitudes, such as preferences and willingness to give the information. However, most researchers apply one of two frameworks: Concern For Information Privacy (CFIP) (Smith et al., 1996) or Internet User's Information Privacy Concerns (IUIPC) (Malhotra et al., 2004). CFIP was the first one to be developed and tested. CFIP regard the information privacy concerns as "individuals' concerns about organizational information

privacy practices." CFIP has four dimensions, including a collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information. Concern for Information Privacy (CFIP) is later revalidated by Stewart and Segars (2002) which has been since accepted as the most generality scales for measuring individuals' concerns toward organizational privacy practices (Smith, Dinev, & Xu, 2011). A few years later, Malhotra et al. (2004) develop a multidimensional scale of Internet Users Information Privacy Concerns , which adopts the scale of CFIP from the original context of offline direct marketing in the Internet context. Focusing on "the individual's" perceptions of fairness/justice the context of information privacy". IUIPC include three dimensions: control, awareness, and collection as shown in Figure 2.9.



Source: (Malhotra et al., 2004)

FIGURE 2.9: Internet Users Information Privacy Concerns

Malhotra et al. (2004) empirically demonstrate that (IUIPC) excelled (CFIP) as a predictor of consumers' reactions to online privacy concerns and show that IUIPC explains more of the variance in a person's willingness to transact than CFIP. In addition Malhotra et al. (2004) claimed that IUIPC is better than CFIP because IUIPC has more factors, a superior internal fit, a powerful relation to Global Information Privacy Concern (GIPC), and a slightly enhanced fitting statistical model..

Thus, as a reliable instrument and framework, the (IUIPC) has been widely applied in different contexts. For example, Buchanan, Paine, Joinson, and Reips (2007) link IUIPC to more specific concerns and protection behaviors of modern privacy-sensitive technologies (e.g., email, e-banking), and Zhang, Wang, and Xu (2011) adapt IUIPC to online social networks (Facebook) information privacy. Thus, it is appropriate to identify information privacy concerns of cloud based e-learning by adopting (IUIPC). Moreover, because IUIPC is based on social contract theory, it is also simply extensible to new types of information privacy (Malhotra et al., 2004).

2.5.1. Collection

The data collection refers to the concern about the number of users' data that is being gathered by organizations. The collection of user data should be limited to the minimum amount of data needed for the purpose for which it is collected (Mather et al., 2009). Thus, data collection is assumed as an important factor of this research which is also a dimension of CFIP and IUIPC.

2.5.2. Control

Control over user data is exceptionally important in the information privacy context and it is often exercised through approval, modification, and the opportunity to opt-in or opt-out (Malhotra et al., 2004) . The idea of the public cloud computing is to outsource increasing business performance and decreasing costs. But this means that data and processes are no longer in the total control of the organization.

Someone else will be dealing with them and both data and processes might reside in different physical locations. Providers, on their side, must ensure the organization has maximum control possible over the data and business processes (Mouratidis et al., 2013). There is a lack of transparency about where such data is, who has rights to use it and what is being done with it (Mowbray & Pearson, 2012). Data proliferation is a feature of public cloud computing, and this happens in a way that may involve multiple parties and is not controlled by the data owners. CSPs ensure availability by replicating data in multiple data centers. Another reason is that it can be difficult to control the exposure of the data that has been transferred to the cloud (Mowbray & Pearson, 2012). However, in the cloud computing environment, concerns arise about how to guarantee collection of minimum amount of data and how to use the data only for an original purpose. Chow et al. (2009) state that due to lack of control in the cloud, organizations have concerns related to the abundance of data and cheap data mining tools, indirect data mining performed by the CSP by analyzing transactional and relationship information. It looks logical to expect that collection of personal information will be a significant factor in information privacy concerns among cloud users.

2.5.3. Awareness

Awareness refers to the degree to which a user is concerned about the awareness of organizational information privacy practices (Malhotra et al., 2004). Based on IUIPC, awareness factor combines two types of justices which are interactional and informational justice. Interactional justice includes issues of transparency and propriety of information made during the enactment of procedures. In contrast, informational justice relates to the disclosure of specific information. According to an online survey among cloud computing users (Quah & Röhm, 2013).Almost half of the end-users are unaware that they are in fact using one or more cloud services themselves already today. While, most of the participants (more than 90%) agree that companies need to inform customers if they store and process personal customer information in the cloud. Cloud computing plays an important role in the future of IT, but the technology's information privacy risks and the apparent user-unawareness necessitates the push for greater transparency of the

technology. According to Malhotra et al. (2004) awareness is a passive dimension of information privacy. Thus, it is believed that the awareness factor will be of the significant effect on user's information privacy concerns.

2.5.4. Social Contract Theory

Social Contract Theory attracts considerable attention in many academic areas including the information privacy (Malhotra et al., 2004). Clients regard the release of personal information as a risky transaction because they become vulnerable to a company's potential opportunistic behavior (Milne & Gordon, 1993). This notion of Social Contract Theory has been applied widely to explain various phenomena including the consumer-firm relationship (Malhotra et al., 2004). This theory has also been used as a conceptual tool for explaining consumer concerns in the context of information privacy (Malhotra et al., 2004; Milne & Gordon, 1993). One of the main principles of Social Contract Theory is that "*norm-generating micro social contracts must be grounded in informed consent, buttressed by rights of exit and voice*" (Dunfee, Smith, & Ross Jr, 1999: P. 19). An equitable exchange involving a long-term relationship should be accompanied by shared understanding about contractual terms and self-control over the course of the relationship (Malhotra et al., 2004). In order to apply this theory in the context of cloud based e-learning system, this research suggests that the collection of users' information is perceived to be fair when the users are granted control over their information, allowing users to access the information when they needed, disclosure to users about where their information is stored, how long the information will be retained, destructing the user's information when the contract is end. The users should also monitor the usage of their information and compliance fair regulations that govern this information as a result, it is possible to characterize the notion of users' information privacy of cloud based e-leering in terms of ten factors: collection, access, control, destruction, retention, compliance, awareness, audit and monitoring, and privacy breaches.

2.5.5. Relationships Between Users Information Privacy of Cloud Based E-Learning and, Trusting Beliefs, Risk Beliefs

A great deal of the literature shows that trust and risk are the two most salient beliefs in information privacy related contexts (Burda & Teuteberg, 2014; Gashami et al., 2014; Malhotra et al., 2004; Sheehan & Hoy, 2000; Widjaja & Chen, 2012). Trusting beliefs are defined as the degree to which people believe a firm is dependable in protecting user's personal information. A general consensus in the trust-risk literature shows that personal concerns influence, to some extent, trusting beliefs and risk beliefs (Malhotra et al., 2004). In the context of this research, implies of user's tendency to worry about information privacy will influence how the person perceives a specific situation in which cloud based e-learning requests personal information. More specifically, cloud based e-learning users with a high degree of information privacy concerns are likely to be low on trusting beliefs and high on risk beliefs. Thus, as depicted in Figure 2.10. We propose that the information privacy concerns of cloud based e-learning will influence trusting beliefs negatively and risk beliefs positively

2.6. The Proposed Conceptual Framework

Since the 1996s, several of conceptual models and measurement scales for information privacy concerns have been developed (Malhotra et al., 2004; Smith et al., 1996). However, these models have been developed and tested in particular contexts such as (offline, direct, marketing, and Internet). Therefore, one can argue whether these models and measurement scales of information privacy concerns can be used and interpreted within different contexts in the same way that they have been interpreted in the contexts where they are developed. Putting it differently, will the information privacy concerns constructs be relevant if they are implemented in different contexts? Furthermore, even the studies that have attempted to measure information privacy concerns in different contexts from those in which the scales were developed have

employed the same constructs and scales without recognizing or considering the effect of new factors on the new contexts that have been not measured yet.

Thus, this research proposes additional factors based on the literature review that has identified the constructs of cloud computing information privacy. The literature review identifies seven key constructs which are access compliance, storage, retention, destruction, audit and monitoring, and information privacy breaches. This research also adopts the three constructs from (IUIPC) which are data collection control and awareness. The proposed model posits that data collection control, awareness, access, compliance, storage, retention, destruction, audit and monitoring, and information privacy breaches all have a positive significant effect on information privacy concerns of cloud based e-learning. Furthermore, the information privacy concerns of cloud based e-learning effect positively on risk beliefs and effect negatively trust as shown in Figure 2.10. To the best of our knowledge, this is the first proposed conceptual framework that has conceded all those factors in a single framework.

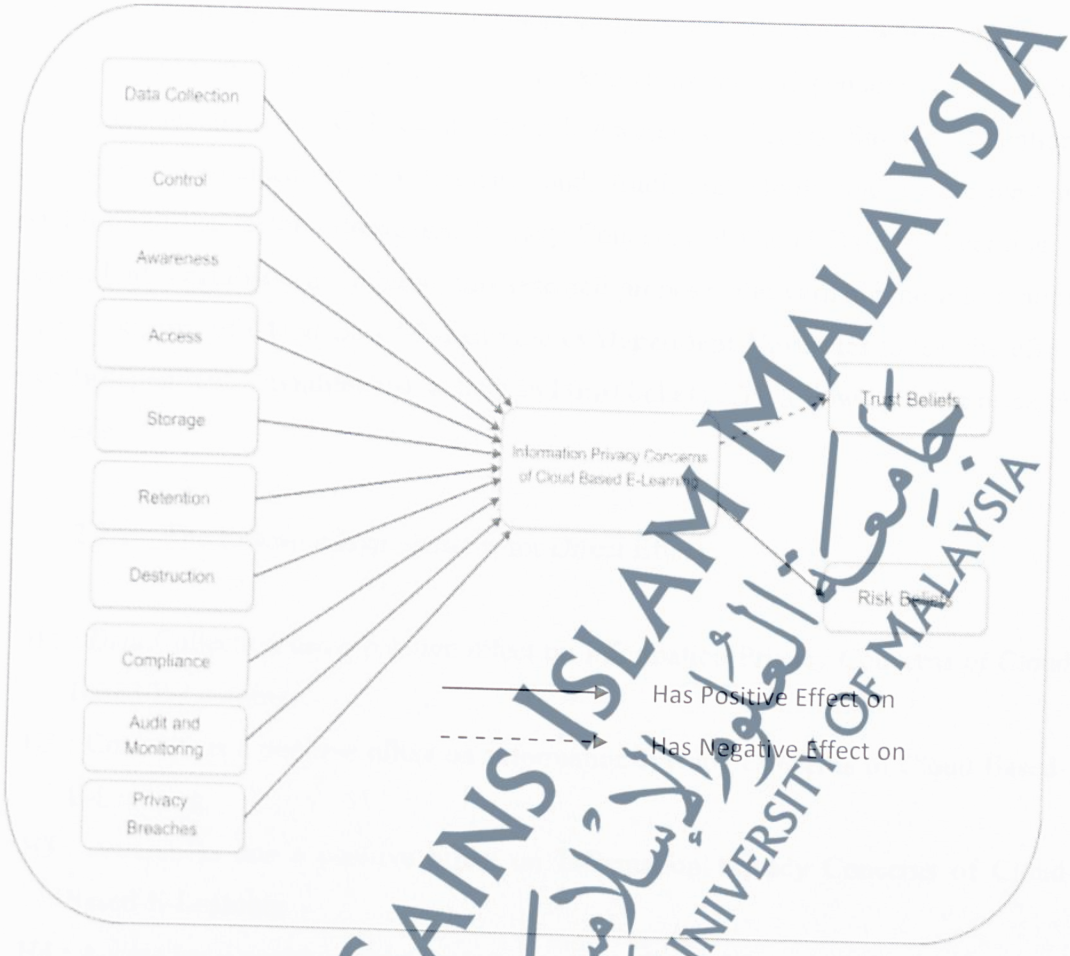


FIGURE 2.10: The Proposed Information Privacy Framework for Cloud Based E-Learning Users

2.7. Research Hypotheses

In order to test the relationships between the variables of conceptual framework, this research proposes several hypotheses. Theses hypotheses are used to answer the research question: how significant are the various factors in influencing on users' information privacy cloud based e-learning. The collected data is analyzed, and the results will indicate whether the hypotheses are confirmed or not. If the hypotheses are confirmed, the statement of the research is supported. In most cases, researchers

investigate a variable known as the dependent variable and observe how it is influenced by modifications in other variables; these are known as the independent. Thus, in this research, the factors: Data Collection, Control, Awareness, Access, Storage, Retention, Destruction, Compliance, privacy Breaches and, Audit and Monitoring are **Dependent Variables** and the factor Information Privacy Concerns of Cloud Based-E-Learning is **Independent Variables.** In addition, this research proposes the variable the Information Privacy Concerns of Cloud Based-E-Learning as **Dependent Variables** to test the effect to two **Independent Variables** risk beliefs and trust beliefs. The following is the research hypothesis.

2.7.1. The Research Hypothesizes for Direct Effect

H1 : Data Collection has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H2 : Control has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H3 : Awareness has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H4 : Access has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H5 : Storage has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H6 : Retention has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H7 : Destruction has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H8 Compliance has a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H9 : Audit and Monitoring have a positive effect on Information Privacy Concerns of Cloud Based-E-Learning.

H10 : Information privacy Breaches has a positive effect Information Privacy Concerns of Cloud Based-E-Learning.

H11 : Information privacy concern of Cloud Based-E-Learning has a positive effect on Risk Beliefs.

H12 : Information privacy concern of Cloud Based-E-Learning has a negative effect on Trust Beliefs.

2.7.2. The Mediating Test

This research also tests the effect of a mediating variable (Information privacy concern of Cloud Based-E-Learning) in the relationship between an independent variable (Data Collection, Control, Awareness, Access, Storage, Retention, Destruction, Compliance, privacy Breaches and, Audit and Monitoring) and its corresponding dependent variables (Risk Beliefs and trust Beliefs).

2.7.2.1. The Research Hypothesizes for Mediating Test on Risk beliefs

H13 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Data Collection and Risk Beliefs.

H14 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Control and Risk Beliefs.

H15 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Awareness and Risk Beliefs.

H16 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Access and Risk Beliefs.

H17 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Storage and Risk Beliefs.

H18 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Retention and Risk Beliefs.

H19 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Destruction and Risk Beliefs.

H20 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Compliance and Risk Beliefs.

H21 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Audit and Monitoring and Risk Beliefs.

H22 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Information Privacy Breach and Risk Beliefs.

2.7.2.2. The Research Hypothesizes for Mediating Test on Trust Beliefs

H23 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Data Collection and Trust Beliefs.

H24 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Control and Trust Beliefs.

H25 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Awareness and Trust Beliefs.

H26 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Access and Trust Beliefs.

H27 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Storage and Trust Beliefs.

H28 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Retention and Trust Beliefs.

H29 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Destruction and Trust Beliefs.

H30 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Compliance and Trust Beliefs.

H31 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Audit and Monitoring and Trust Beliefs.

H32 Information Privacy Concern of Cloud Based-E-Learning mediates the relationship between Information Privacy Breach and Trust Beliefs.

2.8. Chapter Summary

The aim of this chapter is reviewing literature in the information privacy concerns, cloud computing and e-learning and to understand the gap in the research area. Although there are previous studies exploring the information privacy concerns, there is still lacking in literature as they spotlight the information privacy aspect in general. As far as researcher knowledge, there are limitations of literature that focus of users' information privacy of cloud based e-learning and there appears to be a gap in the literature between cloud based e-learning and user's information privacy concerns.

This research has identified the potential information privacy issues which may have an effect on the information privacy concerns of cloud based e-learning users. Furthermore, this research presents a basic conceptual framework that could be beneficial in enhancing the information privacy in cloud computing by contributing influencing factors on users' information privacy.