CHAPTER FIVE

FINDING AND DISCUSSION

5.0. Introduction

Despite the importance of the user information privacy in shaping the adoption of cloud based e-learning, there is a dearth of research examining the information privacy concerns in the cloud based e-learning context. In this chapter, the results presented in chapter 4 are discussed in more detail. The findings for all hypotheses are discussed based on the relationships between independent and dependent variables. These hypotheses are reviewed and compared with prior researches. Moreover, the Cloud Based E-Learning Users' Information Privacy Framework is presented along with the guide of using the research framework. Finally, this chapter explains the evaluation process and results.

5.1. The Factors That Influence on Information Privacy of Cloud Based E-Learning Users

This research develops information privacy framework for cloud based on e-learning users based on the Social Contract Theory and (IUIPC) as well as the factors likely to influence in information privacy concerns of cloud based e-learning. In this respect, the conceptual framework and the related research hypotheses are proposed. A validated instrument is developed, and then the conceptual framework is tested by means of this instrument. The items are clarified by exploratory factor analysis (EFA). Then, a confirmatory factor analysis using SPSS version 22 for Windows is used to confirm the results from the exploratory factor analysis. Cronbach's alpha and composite reliability test tested all the measurement constructs. Thus, all the items demonstrate a reliability value at the satisfaction level. Structural equation modeling using AMOS version 23 is

employed to investigate the relationship between all constructs. The finding of each hypothesis is described as following,

5.1.1. Direct Effect

This section presents the result of examining the direct effects relationship between the independent and dependent variables.

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

The measurement items for (Control) construct are extracted into three items (questions). The findings reveal that all items relating to this construct are rated high by the respondents and the mean score for all three items is between (5.76) and (5.83), as shown in Table B.1 of Appendix B. The mean score of the three items is higher than 4 (the neutral scale) which suggest that the sample agrees with the control construct. Furthermore, the Cronbach's alpha estimate value of control construct is (0.953) (see Table B.3 in Appendix B), which indicates that this construct has the strong reliability of the measurement item.

In the theoretical framework of this research, the control construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H2 that Control has a positive effect on information privacy concerns with a path coefficient of beta for H2 ($\beta = 0.255$, $p = 0.000$).

The above results show that loses control of cloud based e-learning system had positive and significant relationships with information privacy concerns. The result tends to agree with the findings of the previous research (Malhotra, Kim, & Agarwal, 2004; Yang & Miao, 2008; Zheng, Shi, Zeng, & Lu, 2010). This means; the users are more likely to consider the control factor when they use the cloud based e-learning system. The

findings of this research have approved the cloud based e-learning users can recognize the danger of letting information control out of their hands and storing data with an outside in public cloud computing provider. That happens because the data and processes are no longer in the total control of the cloud based e-learning users., Someone else will be dealing with it, both data and processes might reside in different physical locations. The information could be disclosed or used by the cloud computing provider itself or the third party. In addition, the users' concerns about the potential lack of control and transparency when a third party that holds the data. Thus, the CSPs and universities should consider this issue when they implement cloud based e-learning system to increase the levels of information privacy. CSPs must ensure that users and education institution have the possible maximum control over the users' data.

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

The measurement items for (Awareness) construct are extracted into three items (questions). The findings reveal that all items relating to this construct is rated high by the respondents and the mean score for all three items was between (5.84) and (5.9), as shown in Table B.1 of Appendix B, The mean score of all the items is higher than 4 (the neutral scale) which suggest that the sample agree with the Awareness concern. Furthermore, the Cronbach's alpha estimate value of Awareness construct is (0.959) (see Table B.3 in Appendix B), which indicates that this construct has the strong reliability of the measurement item.

In the theoretical framework of this research, the awareness construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H3 that Awareness has a positive effect on information privacy concerns with a path coefficient of beta for H3 ($\beta = 0.171$, $p = 0.005$). The result tends to agree with the findings previous research Malhotra et al. (2004); Quah and Röhm (2013).

The above results show that Awareness factor had a positive effect on information privacy concerns of cloud based e-learning system. That is because it is very important for the users to be there are clear and obvious privacy policies for the cloud based e-learning system. In addition, the users are aware the education institutions who want to collect users' information must tell them what information they want to collect, how they want to use it, how long they will keep it, with which they will share it, and any other uses they intend for the information. They must also notify users if they want to make a change in how the information is used. Thus, the users of cloud based e-learning system should be aware of the privacy compliance requirements, applicable laws, regulations, standards, contractual commitments that govern this information.

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

The measurement items for (Access) construct were extracted into three items (questions). The findings revealed that all items relating to this construct was rated high by the respondents and the mean score for all three items was between (5.9) and (5.97), as shown in Table B.1 of Appendix B. The mean score of the all items was higher than 4 (the neutral scale) which suggested that the sample agreed with the Access concern. Furthermore, the Cronbach's alpha estimate value of Access construct was (0.930) (see Table B.3 in Appendix B), which indicated that this construct had the strong reliability of the measurement item.

In the theoretical framework of this research, the Access construct was conceptualized as independent variables, while an information privacy concern was a dependent variable. As a result, the findings confirmed and supported the hypothesis H4 that Access has a positive effect on information privacy concerns with a path coefficient of beta for H4 ($\beta = 0.175$, $p = 0.003$). The result tends to agree with the findings previous research (Ghorbel, Ghorbel, & Jmaiel, 2017; Mather, Kumaraswamy, & Latif, 2009; Mouratidis, Islam, Kalloniatis, & Gritzalis, 2013; Mowbray & Pearson, 2012; Pearson, 2009).

In summary, the above results show that Access factor has a positive effect on information privacy concern of cloud based e-learning. The results also suggest that users have a strong concern about cloud based e-learning system regarding this factor. That is because the users of cloud based e-learning system are concern about how they can access to their information and how the educational institutions to comply with their requests. Because also, how to prevent others from unauthorized access and misuse the users' data especially in public cloud.

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

Four items (questions) are used to measure the Storage construct. The measurement item (I am concerned if the data of cloud based e-learning system transferred without the knowledge of my universities) (ST3) is dropped due to low factor loading (as shown Table B.7 in Appendix B). However, the mean scores for the rest three items are greater than 4 andwere between (5.95) and (6.6), which suggest that the respondents are agreeable to the three measurement variables. It can, therefore, be implied from these findings that storage factor affects on privacy concern towards using cloud based e-learning. The Cronbach's alpha reliability estimates for storage construct is (0.892), which suggested good internal consistency.

In the theoretical framework of this research, the Storage construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H5 that Storage has a positive effect on information privacy concerns with a path coefficient of beta for H5 (β = 0. 203, p= 0.000). The result tends to agree with the findings previous research (Mather et al., 2009; Pearson, 2009; Pearson & Benameur, 2010; Singh & Goel, 2015).

The above results show that Storage factor has a positive effect on information privacy concerns of cloud based e-learning system. The results also suggest that users

have a strong concern about cloud based e-learning system regarding the location of their information. The location of information in the cloud has significant effects on the privacy and confidentiality protections of information and on the privacy obligations. The users who use the applications provided by the SaaS and process their data in public cloud do not know where the data is stored or is it transferred to another data center in another country. That is because; the users' data may have more than one legal location at the same time with differing legal consequences. In addition, many cloud computing providers are technically able to perform data mining techniques to analyze user data.

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

The measurement items for Retention construct are extracted into three items (questions). The findings revealed that all items relating to this construct are rated high by the respondents and the mean score for all three items is between (5.97) and (6.1), as shown in Table B.1 of Appendix B. The mean score of the all items is higher than 4 (the neutral scale) which suggest that the sample agree with the Retention concern. Furthermore, the Cronbach's alpha estimate value of Retention construct is (0.957) (see Table B.3 in Appendix B), which indicates that this construct had the strong reliability of the measurement item.

In the theoretical framework of this research, the Retention construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H6 that Retention has a positive effect on information privacy concerns with a path coefficient of beta for H6 ($\beta = 0.171$, $p = 0.008$). The result tends to agree with the findings previous research (Mather et al., 2009; Singh & Goel, 2015).

The above results show that Retention factor had positive effect on information privacy concern of cloud based e-learning. That is because, there are concerns of cloud based e-learning users about how long the data will be stored in the cloud. It is important

for the users to know how much time they can access their data on the cloud. The users' data can be more at risk from privacy breaches if the data remain in the cloud for long periods because the data exposure time is much greater. In the traditional IT environment, users or educational institutions usually own and manage the data. But if data is to be migrated into cloud, it should be considered on that how to maintain the data ownership. Therefore, the educational institutions ownership rights over the data must be firmly established in the service contract. The contract should state clearly that the educational institutions retain ownership over all their data.

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

The construct Destruction is measured through four items and the item (I am concerned with is how my university recognizes that the cloud service providers didn't retain additional copies) (DES3) is dropped due the low communalities which is less than (0.5) as shown in Table B.4 in Appendix B. The results show that the mean rating for the remained three items of this construct is between (5.57) and (5.74) and are greater than 4 (neutral point) as shown in Table B.1 of Appendix B which suggest that the respondents are agreeable to the measurement variable. In addition, the construct also shows an acceptable level of internal consistency of measurement items with (0.867) reliability statistics, as shown in Table B.3 in Appendix B. Although this value is above the strict cut off point of this research (> = 0.7), it is lower compared to other constructs.

In the theoretical framework of this research, the Destruction construct is conceptualized as independent variables, while an information privacy concern was a dependent variable. As a result, the findings confirm and support the hypothesis H7 that Destruction has a positive effect on information privacy concerns with a path coefficient of beta for H7 (β = 0. 185, p= 0.007). The result tends to agree with the findings previous research (Mather et al., 2009; Mowbray & Pearson, 2012; Singh & Goel, 2015).

In summary, the above results show that Destruction factor has positive and significant relationships with information privacy concerns of cloud based e-learning. The results also suggest that users have a concern about cloud based e-learning system regarding destruction factor.

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

The measurement items for (Compliance) construct are extracted into three items (questions). The findings reveal that all items relating to this construct is rated high by the respondents and the mean score for all three items is between (6.10) and (6.21), as shown in Table B.1 of Appendix B. The mean score of the all items is higher than 4 (the neutral scale) which suggest that the sample agree with the Compliance concern. Furthermore, the Cronbach's alpha estimate value of Compliance construct is (0.930) (see Table B.3 in Appendix B), which indicate that this construct has the strong reliability of the measurement item.

In the theoretical framework of this research, the Compliance construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H8 that Compliance has a positive effect on information privacy concerns with a path coefficient of beta for H8 ($\beta = 0.148$, $p = 0.007$). The result tends to agree with the findings previous research (Gellman, 2012; Mouratidis, Islam, Kalloniatis, & Gritzalis, 2013; Mowbray & Pearson, 2012; Singh & Goel, 2015; Zhou, Zhang, Xie, Qian, & Zhou, 2010).

The above results show that compliance factor had positive and significant relationships with information privacy concerns. That is because, one of the most common compliance issues facing an organization is different regulations of data location. The users' data in the public cloud usually has more than one legal location at the same time with differing legal consequences. When data crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise concerns

about information privacy. Moreover, the characteristic of many cloud computing services is that detailed information about the location of an organization's data is unavailable or not disclosed to the service subscriber. This situation makes it difficult to ascertain whether legal and regulatory compliance requirements are being met. In contrast, if the cloud computing providers will expose themselves to the laws of all countries from which the services are used, it could be potentially a heavy burden indeed.

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

The measurement items for (Audit and Monitoring) construct is extracted into four items (questions). The measurement item (It is very important to me if my university audits for compliance with privacy and security policies and procedures) with code name (AM4) is dropped due low factor loading (less than 0.6). While the measurement item (It is very important to me what specific regulatory requirements are applicable in cloud based e-learning system of my university) with code name (AM2) is rated highly among the respondents of the survey with the mean score for this construct is (6.19). The mean scores for the three items are greater than 4 (neutral point) and the mean ratings for the three items are between (6.00) and (6.19) as shown in Table B.1 of Appendix B, which suggest that the respondents are agreeable to the measurement variables. It can, therefore, be implied from these findings that audit and monitoring affect respondents' information privacy concerns towards using cloud based e-learning system. Cronbach's alpha coefficient value for audit and monitoring is (0.869) as shown in Table B.3 in Appendix B.

In the conceptual framework of this research, the Audit and Monitoring construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H9 that Audit and Monitoring has a positive effect on information privacy concerns with a path coefficient of beta for H9 (β = 0. 163, p= 0.014). The finding tends to agree with the

findings previous researches (Singh & Goel, 2015; Zhou, Zhang, Xie, Qian, & Zhou, 2010).

In summary, the above results show that audit and monitoring had positive and significant relationships with information privacy concerns cloud based e-learning. The results also suggest that users have a strong concern about cloud based e-learning system regarding audit and monitoring. For the reason that the educational institutions that adopt cloud based e-leaning system creates a new environment that is complex to audit and monitor. The traditional monitoring and audit tools are not as effective in cloud environments as they are in monitoring the performance of internally. Education institutions need to monitor not only actual levels of performance but also enable them to analysis the cause of any problems occur. Also, they need to monitor how changes in policies that control cloud computing resources and how cloud resources are being used.

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

All the measurement items for (Information privacy breaches) construct are extracted into three items (questions). The findings reveal that all items relating to this construct are rated high by the respondents and the mean score for all three items is between (6.11) and (6.17), as shown in Table B.1 of Appendix B. The mean score of the all items is higher than 4 (the neutral scale) which suggest that the sample agreed with the Information Privacy Breaches concern. Furthermore, the Cronbach's alpha estimate value of Information Privacy Breaches construct (BP) (0.922) (see Table B.3 in Appendix B), which indicate that this construct had the strong reliability of the measurement item.

In the theoretical framework of this research, the information privacy breaches construct is conceptualized as independent variables, while an information privacy concern is a dependent variable. As a result, the findings confirm and support the hypothesis H10 that Information Privacy Breaches has a positive effect on information privacy concerns with a path coefficient of beta for H10 (β = 0.214, p= 0.005). The

finding tends to agree with the findings previous researches (Mather et al., 2009; Mouratidis et al., 2013; Singh & Goel, 2015).

In summary, the above results show that information privacy breaches have positive and significant relationships with information privacy concerns of cloud based e-learning. That is because, the data from various users and organizations store together in a cloud environment, any privacy breaches of the cloud environment will potentially attack the data of all the users. A single incident could expose information from many users. The cloud computing environment becomes a high value target for the information privacy breaches. Cloud based e-learning users need to be vigilant in understanding the risks of data breaches in this new environment. Moreover, they need to ensure that the cloud service provider notifies the users and education institution when a breach occurs, and who is responsible for managing the breach notification process, how is the contract enforced and how is it determined who is at fault.

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

The Risk Beliefs construct is measured by four items and the measurement item (There would be too much uncertainty associated with giving the information to cloud based e-learning system of my university) with code name (RB1) is deleted from the analysis due to the low of factor loading (less than 0.6) as shown Table B.7 of Appendix B. The results reveal that the mean ratings of remained three items of this construct were higher than the neutral point, which confirmed participants' acceptance of measured items. In short, the average mean score of all measurement items of this construct was between (5.78) and (6.03) as shown Table B.1 of Appendix B. In addition, the reliability statistics of clarity construct (as shown Table B.3 in Appendix B) revealed that Cronbach's alpha reliability is (0.920), which suggested adequate reliability of this construct's items.

In the theoretical framework of the present research, an information privacy concern of cloud based e-learning is conceptualized as independent variables, while a risk belief is the dependent variables. The findings show that the information privacy concern of cloud based e-learning factor has a statistically significant and positive relationship with risk beliefs. It confirms and supports the hypotheses H11 that information privacy concern of cloud based e-learning has a positive effect on risk beliefs with a paths coefficient of H11 (β = 0.360, p= 0.000). That means cloud based e-learning system users are concern about information privacy risk when they use the system. While the risk belief is commonly thought of as the felt uncertainty regarding the possible negative consequences of adopting a product or service, the results of this study confirmed the users believe there is an information privacy risk of using cloud based e-learning system. That is because they do not sure about consequences of using this system. However, the users feel more comfortable with risk when they have more control over their information rather than someone else controls it. In order to reduce the risk beliefs of the cloud based e-learning users, it should the education institutions take the actual steps to reduce the information privacy issues.

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

The Trust construct is measured by five items. While the trust beliefs construct negative effect, the five items are reversed coded. The measurement item (Cloud services provider is in general predictable and consistent regarding the usage of the information) with code name (TB4) is deleted from the analysis due low communalities (less than 0.5) as shown Table B.4 in Appendix B. The overall mean score of all items of this construct is between (2.12) and (2.17), which suggest that respondents has reservations about their trust in cloud based e-learning system. This is evident from the low mean rating which might suggest that respondents are concerned about the privacy of the cloud based e-learning system which reflects on their trust belief of cloud services provider. In addition, the reliability statistics of the trust belief construct (Table B.3 in Appendix B) indicated

(0.921) Cronbach's alpha reliability for this construct, which shows the good internal consistency of measurement items of this construct.

In the theoretical framework of the present research, an information privacy concern is conceptualized as independent variables, while a trust belief is the dependent variables. The finding also shows that the privacy concerns factor has a statistically significant and negative relationship with trust beliefs. It also confirms and supports the hypothesis H12 that information privacy concerns factor has a significant negative relationship with trust beliefs with a paths coefficient of H12 (β = - 0.365, p= 0.000).

The above results show that information privacy concerns in the cloud based e-learning system has negative and significant relationships with user trust which mean less privacy concern results in high levels of users' trust (see Table 5.1). Information privacy literature shows the important positive role played by trust, and the findings from multiple studies concur on trust being the most salient beliefs of information privacy (Cespedes & Smith, 1993; Malhotra et al., 2004). However, from the finding of this study, there is a negative relation between information privacy concerns of cloud based e-learning system and trust beliefs of the users. Thus, the users cannot trust completely on the provider. Because they have a concern about their information privacy issues on cloud based e-learning system.

5.1.2. Test of Mediation Effect

This section presents the result of examining the mediator of information privacy concerns between the independent (control, awareness, access, storage, retention, destruction, compliance, audit and monitoring and privacy breaches) and dependent variables (Risk Beliefs and Trust Beliefs).

5.1.3. Test of Mediation Effect of Information Privacy Concerns in The Relationship with Risk Beliefs

As shown earlier, hypothesis (H14) explains the mediation effect of information privacy concerns in the relationship between the control and risk beliefs. As outlined in Table 4.10, the information privacy concern does mediate the relationship between the control and risk beliefs. Thus, this hypothesis is supported (see Table 5.1).

The hypothesis representing the mediation effect of information privacy concerns in the relationship between awareness and risk beliefs H15 is supported (see Table 5.1), the complete mediation occurs since indirect effect < Direct effect as shown in Table 4.11.

The hypothesis (H16) explaining the mediating role of information privacy concerns between access and risk beliefs is rejected (see Table 5.1). According to the results presented in Table 4.12, it is no mediation found in the hypothesized (Since indirect effect < Direct effect).

Hypothesis (H17) presents the mediation effect of information privacy concerns in the relationship between storage and risk beliefs. As hypothesized, storage has an indirect positive effect on risk beliefs through its influence on information privacy concern is supported (see Table 5.1). As shown in Table 4.13 indirect effect < Direct effect.

The hypothesis (H18) explaining the mediating role of information privacy concerns between retention and risk beliefs Results in Table 4.14 indicate that the complete mediation occurs, and the hypothesis was supported (see Table 5.1).

The hypothesis (H19) explaining the mediating role of information privacy concerns between destruction and risk beliefs is rejected (see Table 5.1). According to the

results presented in Table 4.15, there is no mediation found in the hypothesized (Since indirect effect < Direct effect).

The hypothesis (H20) explaining the mediating role of information privacy concerns between compliance and risk beliefs. Results in Table 4.16 indicate that the complete mediation occurs, and the hypothesis was supported (see Table 5.1).

The hypothesis (H21) explains the mediating role of information privacy concerns between audit and monitoring and risk beliefs. According to the results presented in Table 4.17, it has been found that complete mediation occurs. Thus, this hypothesis was supported (see Table 5.1).

The hypothesis (H22) explaining the mediating role of information privacy concerns between information privacy breaches and risk beliefs is rejected (see Table 5.1). According to the results presented in Table 4.18, there is no mediation found in the hypothesized (Since indirect effect < Direct effect).

5.1.4. Test of Mediation Effect of privacy Concerns in The Relationship with Trust Beliefs Information

As shown earlier, hypothesis (H24) explained the mediation effect of information privacy concerns in the relationship between the control and trust beliefs. As outlined in Table 4.19, the information privacy concern does mediate the relationship between the control and trust beliefs. Thus, this hypothesis was supported (see Table 5.1).

The hypothesis representing the mediation effect of information privacy concerns in the relationship between awareness and trust beliefs H25is supported (see Table 5.1), the complete mediation occurs since indirect effect < Direct effect as shown in Table 4.20.

Hypothesis (H26) explains the mediation effect of information privacy concerns in the relationship between access and trust beliefs. As hypothesized, Access has an indirect negative effect on trust beliefs through its influence on information privacy concern was supported (see Table 5.1). As shown in Table 4.21 indirect effect < Direct effect.

The hypothesis (H27) explaining the mediating role of information privacy concerns between storage and trust beliefs. Results in Table 4.22 indicate that the complete mediation occurs, and the hypothesis was supported (see Table 5.1).

The hypothesis (H28) explaining the mediating role of information privacy concerns between retention and trust beliefs. Results in Table 4.23 indicate that the complete mediation occurs, and the hypothesis was supported (see Table 5.1).

The hypothesis (H29) explaining the mediating role of information privacy concerns between destruction and trust beliefs is rejected (see Table 5.1). According to the results presented in Table 4.24, there is no mediation found in the hypothesized (Since indirect effect < Direct effect).

The hypothesis (H30) explaining the mediating role of information privacy concerns between compliance and trust beliefs is rejected (see Table 5.1). According to the results presented in Table 4.25, there is no mediation found in the hypothesized (Since indirect effect < Direct effect).

The hypothesis (H31) explains the mediating role of information privacy concerns between audit and monitoring and trust beliefs. According to the results presented in Table 4.26, it has been found that complete mediation occurs. Thus, this hypothesis is supported (see Table 5.1).

The hypothesis (H32) explaining the mediating role of information privacy concerns between information privacy breaches and trust beliefs is rejected (see Table

5.1). According to the results presented in Table 4.27, there is no mediation found in the hypothesized (Since indirect effect < Direct effect).

TABLE 5.1: Results of Testing the Hypotheses

	Hypotheses	Result
H2	Control has a positive effect on information privacy concerns.	Supported
H3	Awareness has a positive effect on information privacy concerns.	Supported
H4	Access has a positive effect on information privacy concerns.	Supported
H5	Storage has a positive effect on information privacy concerns.	Supported
H6	Retention has a positive effect on information privacy concerns.	Supported
H7	Destruction has a positive effect on information privacy concerns.	Supported
H8	Compliance has a positive effect on information privacy concerns.	Supported
H9	Audit and Monitoring have a positive effect on information privacy concerns.	Supported
H10	Information privacy Breaches has a positive effect on information privacy concerns.	Supported
H11	Information privacy concern has a positive effect on risk beliefs.	Supported
H12	Information privacy concern has a negative effect on trust beliefs.	Supported
H14	Control has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H15	Awareness has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H16	Access has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Not Supported
H17	Storage has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H18	Retention has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H19	Destruction has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Not Supported

H20	Compliance has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H21	Audit and monitoring have an indirect positive effect on risk beliefs through its influence on information privacy concern.	Supported
H22	Information privacy breach has an indirect positive effect on risk beliefs through its influence on information privacy concern.	Not Supported
H24	Control has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H25	Awareness has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H26	Access has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H27	Storage has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H28	Retention has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H29	Destruction has an indirect negative effect on trust beliefs use through its influence on information privacy concern.	Not Supported
H30	Compliance has an indirect negative effect on trust beliefs through its influence on information privacy concern.	Not Supported
H31	Audit and monitoring have an indirect negative effect on trust beliefs through its influence on information privacy concern.	Supported
H32	Information privacy breach has an indirect negative effect on trust beliefs through its influence on information privacy concern	Not Supported

5.2. Information Privacy Framework for Cloud Based E-Learning Users

The information privacy framework of cloud based e-learning users is constructed based on the Social Contract Theory as well as Internet Users Information Privacy Concerns framework (IUIPC) (Malhotra et al., 2004) and based on a broad literature review that has identified the information privacy issues of cloud computing. The literature identifies nine factors. These factors are clarified by exploratory factor analysis and measured again by confirmatory factor analysis to validate the framework. Structural

equation modeling is used to test pathways between the factors. The analysis result indicates that the factors show a high degree of the Unidimensionality, convergent validity, discriminant validity, and reliability. The findings indicate that the factors Control, Awareness, Access, Storage, Retention, Destruction, Compliance, Audit and Monitoring, and Privacy Breaches have a positive effect on information privacy concerns of cloud based e-learning users. Besides, information privacy cloud based e-learning concern factor has a positive effect on risk beliefs and negative effect on trust belief. Figure 5.1 illustrates The Proposed Information Privacy Framework for Cloud Based E-Learning Users.

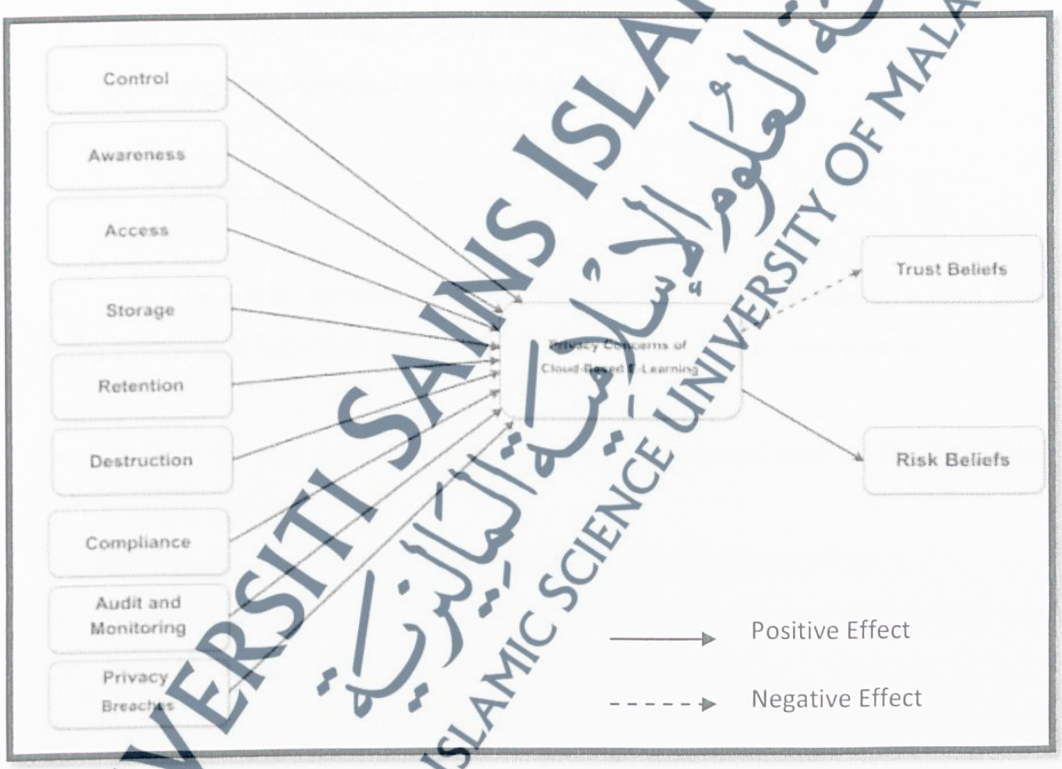

FIGURE 5.1: The Proposed Information Privacy Framework for Cloud Based E-Learning Users

5.3. The Guide of Using Information Privacy Framework for Cloud Based E-Learning Users

This section demonstrates the guide of using of cloud based e-learning users' information privacy framework.

a) Control

The loss control on users' data of cloud based e-learning system.

- Ensure the users' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- Maximize effectiveness of secure data transfers.
- Increase control over information disclosure.

b) Awareness

The users' awareness of the information privacy issues of cloud based e-learning system and how their information is collected, are used and shared.

- Disclose the way the data are collected, processed, and used on the cloud based e-learning system.
- increase the clarity and conspicuous disclosure of privacy policy
- Increase the awareness of how the users' information is used on the cloud based e-learning system.
- Ensure the Cloud Service Providers' privacy policy and practices are effectively communicated and understood
- Increase awareness of data ownership.

c) Access

The access rights of the users and complying with the user's request for add, modify and delete. Also, prevent the others from unauthorized access and misuse over the data.

- Optimize access controls
- Minimize third party access to information
- Minimize unnecessary access to information
- Provide the users with access to all personal information on cloud based e-learning system.
- Comply with all user requests (Add, Modify, and Delete).
- Ensure that all of users' information has been deleted in the cloud based e-learning system.

d) Storage

The physical location of where the data is stored.

- Maximize effectiveness of secure data transfers to another cloud centre in another country.
- Disclose where is the data of cloud based e-learning system stored in the cloud.
- Notify the users when their data is transferred
- Minimize the commingle users' data with data from other organizations that use the same cloud services provider.

e) Retention

The period for storing users' data in cloud computing.

- Determine retention period.
- Optimize the retention policy that governs users' information in the cloud based e-learning system
- State clearly that the retain ownership over all its data.
- Ensure the ownership of the data.

f) Destruction

The process of delete users' data at the end of the retention period.

- Ensure the destroying of users' data at the end of the retention period.
- Ensure that its data is destroyed at the right point and is not available to other cloud users.
- Ensure the cloud service providers didn't retain additional copies.
- Ensure the destruction completely erases the data.

g) Compliance

The list of applicable laws, regulations, standards and contractual commitments that govern cloud based e-learning system data.

- Ensure there are clear privacy compliance requirements govern the information in cloud based e-learning system.
- Ensure there are clear applicable laws, regulations, standards, and contractual commitments that govern information in cloud based e-learning system.
- Optimize the existing privacy compliance requirements to be suitable for by cloud computing environment.

h) Audit and Monitoring

How users and institutions can monitor the cloud based e-learning system and maintain the assurance that privacy requirements are met.

- Ensure the different levels of requirements for different sets of users in cloud based e-learning system of my university.
- Optimize the regulatory requirements are applicable in cloud based e-learning system of my university.
- Provide assurance to the users that privacy requirements are met.
- Optimize the audits for compliance with privacy and security policies and procedures.

i) Privacy Breaches

To ensure that the cloud based e-learning system will notify the users when a breach occurs, and who is responsible for managing the process of notifying breaches.

- Ensure how privacy breaches have occurred in cloud based e-learning
- Ensure how the cloud service provider notifies users when a breach occurs.
- Determine who is responsible for managing the breach notification.

5.4. The Validation of Framework

Validation is the process of ensuring that the model is sufficiently accurate for its purpose (Carson, 1986). The validation process is an essential step to obtain the expert perspective about the research findings. After the research framework is developed, it is important to evaluate whether the framework reflects the needs of the information privacy

of cloud based e-learning users. This section presents validation process, selection of experts' panel and reports the findings validation results.

5.4.1. The Validation Process

The main aims of the validation are to obtain opinion of a panel of experts to determine the degree to which the research framework and research framework guides are clear, sufficient, understand, usable and applicable. The validation is conducted after the research framework is developed and experts are invited to participate to obtain their opinion.

The validation survey is organized by explaining in brief the aim of the research, the construct of research framework, the proposal framework, explanation of the research factors, and the guide of using this framework. The questionnaire contains eight questions using a five-point Linker (Strongly Agree, Agree, Neither Agree nor Disagree, Disagree and Strongly Disagree). The validation survey can be found in Appendix C. This research invites five experts to participate in validating the research framework. The survey is sent to the experts by e-mail.

5.4.2. The Panel of Experts

Five experts responded to the invitation of the validation survey. All the experts have an academic and research background and they are working in public universities in Malaysia. Expert 1 is Senior Lecture and Head of Learning and Teaching Innovation at University of Malaya with experience 3 years. Expert 2 is Associate Professor and Deputy Director (ICT Support) in Universiti Kebangsaan Malaysia (UKM) with experience more than 10 years. She is the head of Personalized Education Research Group. Her research area includes E-Training and E-Learning Design, Development, Testing, Evaluation, Assessment and Modeling. Expert 3 is Associate Professor and Director of Teaching and Learning Centre at Universiti Teknikal Malaysia Melaka (UTeM) with experience 3 years. Expert 4 is a lecturer and Head of the Department for

Centre of Academic Development, Universiti Tun Hussein Onn Malaysia (UTHM). Expert 5 is an Associate Professor and the Head of e-Learning Centre for Academic Planning, Development and Quality, Universiti Malaysia Terengganu (UMT) with experience more than 15 years.

5.4.3. Validation Results

This section presents experts' opinion on the research framework and guidelines. All experts' responses are presented in APPENDIX D. The section is organized into sub-sections according to the survey questions.

5.4.3.1. The Clarity of Framework

In order to insure the clearly the framework to be easily adopted, it is important to validate if the factors define clearly. Hence, the question (to what extent do you agree the framework factors define clearly?) is addressed. The results show that one of the experts strongly agrees and four experts agree that the framework factors are defined clearly. This result confirms that the majority of the feedbacks from the experts are positive with regards to clarity of the framework factors.

5.4.3.2. The Sufficiently of Framework

The experts agree that the elements of framework are sufficient and be able to ensure the information privacy of cloud based e-learning. Two experts strongly agree, and three experts agree by answering the question (to what extent do you agree that the elements of the framework are sufficient to ensure the information privacy of cloud based e-learning?).

5.4.3.3. Representing the Current Information Privacy Issues

This validation survey also finds that the research framework guides represent the current information privacy issues. The result is (one of the experts strongly agree and, three of them agree). This result of the question (to what extent do you agree that the guide the guide of the framework represents current information privacy issues of cloud based e-learning?). The expert 4 comments that *(Should consider also copyright issues. Ownership of the materials or resources available via cloud. Flexible rules or procedures for education purposes should not be jeopardize)*. However, in this research, the access and retention factors consider the ownership issue as explained in using guide and subsection (2.3.5.4).

5.4.3.4. The Appropriately of Framework

The proposed framework consists of nine factors; these factors represent the various information privacy issues of cloud based e-learning. Thus, it is essential to validate if appropriate to include these factors in one framework. Hence, this research addresses the question (to what extent do you agree that it is appropriate to include these factors in one framework?) to the experts. The result shows that two experts strongly agree and three of experts agree to include these factors in one framework. The result has been proved that it is very appropriate to include the nine factors in the framework.

5.4.3.5. Increasing the Information Privacy Protection

This research has proposed framework in order to improve the information privacy protection of cloud based e-learning. To ensure this objective is met, the question (to what extent do you agree that the framework helps educational institutions to increase the information privacy protection of cloud based e-learning users?) is addressed and the result is (two experts strongly agree and three of them agree).

Based in this result, it has been found that the proposed framework is very helpful to for the users to increase the information privacy protection.

5.4.3.6. The Understandably of Framework Guide

In order to ensure the framework and guidelines are easy to understand, the question (to what extent do you agree that it is easy to understand the framework and guidelines?) is addressed and the result is (one expert strongly agrees, and four experts agree). The result indicates all experts agreed that the framework and guidelines could be easy to understand.

5.4.3.7. The Usability of The Framework

While it is important to ensure the framework can be used by education institutions to be put into practice, the question (To what extent do you agree that the framework usable in practice?) is addressed to the experts and the results are (two experts strongly Agree and three Agree). There is a consensus amongst the experts that in general the framework is usable in practice.

5.4.3.8. The Applicability of The Framework

The survey also validates if the framework and guidelines can be applied in most educational institutions. The result is (two experts strongly agree, two experts agree). On the other hand, the expert 2 comment *(It may or may not apply to most educational institution depending on confirmatory result of the study*). However, the majority of the experts agree that the framework could be applied in the other educational institutions. The summary of the validation questions and results are summarized in the Table 5.2

TABLE 5.2: Evaluation objectives, Question and Results

	Evaluation Objectives	Question	Results
1.	Clarity of framework	To what extent do you agree the framework factors define clearly?	20 % Strongly Agree 80% Agree
2.	The sufficient of framework	To what extent do you agree that the elements of the framework are sufficient to ensure the information privacy of cloud based e-learning?	40% Strongly Agree 60% Agree
3.	Representing the current information privacy issues	To what extent do you agree that the guidelines of the framework represent current information privacy issues of cloud based e-learning?	20 % Strongly Agree 60% Agree
4.	The appropriately of framework	To what extent do you agree that it is appropriate to include these factors in one framework?	40% Strongly Agree 60% Agree
5.	Helps to increase the information privacy protection	To what extent do you agree that the framework helps education institutions to increase the information privacy protection of cloud based e-learning users?	40% Strongly Agree 60% Agree
6.	Understandable	To what extent do you agree that it is easy to understand the framework guidelines?	20% Strongly Agree 80% Agree
7.	Usability	To what extent do you agree that the framework usable in practice?	20% Strongly Agree 80% Agree
8.	The significant of guidelines and the capability to apply	To what extent do you agree that the given guidelines of the framework are significant and likely to apply to most educational institutions?	40 % Strongly Agree 40 % Agree

The result proves the appropriately, easy to understandable, usability, sufficiently, clarity of research framework and guidelines. The validation process by an expert panel has proved the accuracy of study results. We believe that the involvement of such a high expert panel adds weight and rigor to our results.

5.5. Chapter Summary

This chapter has presented the cloud based e-learning users' information privacy framework. In addition, this chapter demonstrates the guide of using of cloud based e-learning users' information privacy framework. The users, educational institution and cloud service providers would be able to understand the information privacy of cloud based e-learning framework. The findings are explored in this chapter. All hypotheses developed in the framework are discussed in relation to literature and find inferences for the future. Results indicate that the control, awareness, access, storage, retention, destruction, compliance, audit and monitoring and, information privacy breaches have a positive significant influence on information privacy concerns while information privacy concern has a negative significant influence on trust beliefs and information privacy concern has a positive significant influence on risk beliefs. Moreover, this chapter presents the validation process and results. The majority of the opinion from the panel expert is positive with regards to appropriately, easy to understandable, usability, sufficiently, clarity of research framework and guidelines.