Security Determinants of the Educational Use of Mobile Cloud Computing in Higher Education

Waleed Alghaith
waalghaith@imamu.edu.sa
Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Saudi Arabia.

Summary
The decision to integrate mobile cloud computing (MCC) in higher education without first defining suitable usage scenarios is a global issue as the usage of such services becomes extensive. Consequently, this study investigates the security determinants of the educational use of mobile cloud computing among universities students. This study proposes and develops a theoretical model by adopting and modifying the Protection Motivation Theory (PMT). The studys findings show that a significant amount of variance in MCC adoption was explained by the proposed model. MCC adoption intention was shown to be highly influenced by threat appraisal and coping appraisal factors. Perceived severity alone explains 37.8% of students "Intention" to adopt MCC applications, which indicates the student's perception of the degree of harm that would happen can hinder them from using MCC. It encompasses concerns about data security, privacy breaches, and academic integrity issues. Response cost, perceived vulnerability and response efficacy also have significant influence on students "intention" by 18.8%, 17.7%, and 6.7%, respectively.

Keywords:
MCC, PMT, Security, adoption, Saudi Arabia.

1. Introduction

This decade has seen the expansion of mobile portable device production, such as smart phones and tablets, as well as the rise of a wide range of mobile operating system suppliers, such as Microsoft, Apple, and Google. Mobile technologies are changing the way we live, work, play, and learn on the Internet. New technologies such as 5G and Wi-Fi 6 provide mobile users with increased coverage, greater download speeds, and less latency to provide better wireless services. Advances in mobile technology are also laying the groundwork for a new age of interactive Internet apps and Internet of Things (IoT) development.

According to the last CISCO report, globally, the total number of mobile subscribers (those who use mobile services) is expected to rise to reach 5.7 billion by 2023. This is equivalent to 71 percent of the world's population in 2023. North America and Western Europe have the highest regional mobile adoption, whereas the Middle East and Africa will have the fastest mobile growth [1]. This revolution in usage, which is due to the revolution in mobile applications, led to the emergence of mobile cloud computing (MCC) as a new shared computing model. MCC can be described as an application that allows data to be transferred from smart mobile devices to be stored and processed on remote cloud servers [2]. MCC changed the way information is presented to students in higher education.

In recent years, the integration of MCC in higher education has gained significant attention. This emerging technology offers numerous benefits to both students and educators, such as increased accessibility to educational resources and improved collaboration. However, the successful implementation of MCC in higher education heavily relies on ensuring robust security measures. Students have constant access to information and study resources when they use mobile Internet on their cell phones. Furthermore, social networking and communication apps enable students to exchange information with their classmates and friends. More significantly, the integrated technologies allow them to access information held in MCC services to solve problems and make decisions. This technology allows students and educators to access educational resources and collaborate on projects from anywhere, at any time. However, concerns about the security of mobile cloud computing have hindered its widespread adoption in higher education.

One of the key determinants of the educational use of mobile cloud computing is data privacy and security [3]. Educational institutions handle vast amounts of sensitive student information, including grades, personal details, and financial records. Furthermore, device security plays a vital role in ensuring the safe use of mobile cloud computing in higher education [4]. Scholars are increasingly emphasizing the importance of individuals in information systems' usage ([3], [4], [5], [6], [7]). Given this reality, we need to understand the determinants of the educational use of mobile cloud computing among students. This raises the following research question: What are the security determinants of the educational use of MCC in higher education? The rest of this paper answers this question by applying the Protection Motivation Theory (PMT) as a potential theory to explain differences in security behavior, particularly in using MCC. This paper is organized as follows: The next section presents a literature review on MCC in general and MCC adoption in

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.10

higher education and the study's theoretical framework, which includes the PMT theoretical approach as the main theory that guides the development of the study model. The third section discusses the development of research hypotheses and the study model. The fourth section describes the study methodology, including its measurements and applied data collection procedures. The fifth section presents the research data analysis and its findings, which cover the reliability and validity of the study instrument and the hypotheses testing results. The sixth section provides a discussion related to the study findings and the proposed study model.

2. Literature review and Theoretical Framework

2.1 Mobile cloud computing

Mobile cloud computing is a revolutionary concept that combines the power of mobile devices with the flexibility and scalability of cloud computing. It refers to the ability to access and use cloud-based applications and services through mobile devices such as smartphones and tablets. This technology has transformed the way we use our mobile devices, enabling us to store, process, and share data seamlessly.

One of the key benefits of mobile cloud computing is its ability to offload computational tasks from mobile devices to remote servers in the cloud. This allows for more efficient use of resources on mobile devices, as they no longer need to perform computationally intensive tasks locally. Instead, these tasks can be executed on powerful servers in the cloud, which can handle them more efficiently [8].

Another advantage of mobile cloud computing is its ability to provide ubiquitous access to data and applications. With this technology, users can access their files, documents, and applications from anywhere at any time. This eliminates the need for physical storage on individual devices and enables seamless collaboration among users [9].

Furthermore, mobile cloud computing offers significant cost savings for both individuals and businesses. By leveraging shared resources in the cloud, users can reduce their hardware costs while still enjoying high-performance capabilities [10]. Additionally, businesses can benefit from reduced maintenance costs as they no longer need to manage complex IT infrastructure locally.

MCC application operate on portable devices and take advantage of the strength and availability of cloud services to fulfil tasks like accelerated cloud computing power and limitless storage [10]. MCC represents the combination and integration of mobile and cloud computing services into a single, seamless model. Although this combination has a number of advantages, it has also increased security and complexity issues [11]. Users' concerns regarding their privacy, security and level of control over their mobile device camera and sensors can greatly limit the idea of using MCC applications [12]. Concerns related to privacy invasion, security vulnerabilities, and loss of control act as significant deterrents for widespread adoption. Privacy is a fundamental right that users expect when using any technology. The idea of having a camera and sensors constantly monitoring their activities raises concerns about potential breaches in personal privacy. Users fear that their private moments might be captured without consent or used for malicious purposes. Security is another major concern for users. With the increasing number of cyber threats and data breaches, individuals are wary of granting access to their mobile device's camera and sensors. They worry about unauthorized access to sensitive information or the possibility of being tracked without their knowledge. Moreover, users also express apprehension about losing control over their mobile devices. Granting access to camera and sensor functionalities may result in third-party apps gaining excessive control over these features, potentially compromising user experience or even leading to physical harm. These concerns significantly limit the idea of using MCC applications. Users are hesitant to embrace these technologies due to fears surrounding privacy invasion, security vulnerabilities, and loss of control over their devices' core functionalities.

In the next section, we delve into a deeper understanding of the determinants of using the MCC, drawing from theoretical perspectives within the field of Information Systems and, in particular, the Protection Motivation Theory.

2.2 Protection Motivation Theory

Human fear is a feeling or passion that is driven by the expectation of evil or the dread of approaching danger; in reaction to fear, humans adopt an emotional state that protects them from danger or a motivational condition that leads them away from something [13]. Scholars noticed that this fear reaction, also known as a fear appeal, may affect attitudes and, as a result, behavior. Rogers [13] developed Protection motivation theory (PMT) to give

conceptual clarity in the field of fear appeals and to explore the relationship between fear appeals and attitude modification. PMT) is a model that seeks to explain how individuals perceive and respond to threats or risks. PMT identified the components of a fear appeal in order to identify the common characteristics that caused attitude change. According to PMT, each component of a fear appeal would trigger a related mental or cognitive mediation process. These mechanisms have an effect on protective motivation in the form of an intention of performing the recommended behavior [13]. Rogers demonstrated in 1983 that these cognitive mediational processes may be divided into two categories: (1) threat appraisal and (2) coping appraisal [14], [15]. Threat appraisal involves evaluating the severity and susceptibility of a potential threat. If an individual perceives a threat as severe and likely to affect them personally, they are more likely to be motivated to take protective action. For example, if someone believes that smoking poses a high risk of developing lung cancer, they may be motivated to quit smoking ([14], [15], [16], [17], [18]). Coping appraisal refers to an individual's assessment of their ability to effectively cope with the perceived threat. If someone believes they have the necessary skills, resources, or support systems in place to deal with the threat, they are more likely to engage in protective behaviors. For instance, if someone believes they have access to effective treatments for a particular disease, they may be more inclined to seek medical help [14], [15].

PMT has been widely applied in various fields such as health promotion campaigns and disaster preparedness efforts. By understanding how individuals perceive threats and their ability to cope with them, practitioners can tailor interventions that enhance motivation for protective actions.

2.3 Hypotheses development

PMT posits that individuals are motivated to protect themselves from potential threats by assessing the severity and vulnerability associated with those threats, as well as the response efficacy and response cost. This theory suggests that people are more likely to engage in protective behaviors if they perceive the threat as severe and themselves as vulnerable to it ([14], [15], [16], [17], [18]).

In the context of mobile cloud computing, this theory suggests that users' decision to adopt or reject this technology is influenced by their perception of its security risks.

Perceived severity, perceived vulnerability, Response efficacy and Response cost are four key determinants of the adoption of MCC in higher education. Perceived severity refers to the perceived impact or consequences of a security breach, while perceived vulnerability refers to the perceived likelihood of a security breach occurring. When it comes to the educational use of MCC, students and educators may perceive the severity of a potential security breach as high due to the sensitive nature of educational data that could be compromised. For example, if personal information or academic records were accessed by unauthorized individuals, it could have serious implications for both students and institutions. Scholar found that perceived severity is positively related to security, privacy and personal data protection behaviour and negatively on MCC adoption ([19], [20]). Similarly, perceived vulnerability plays a crucial role in determining the level of security associated with mobile cloud computing [20]. In the context of mobile cloud computing, it relates to how users perceive the security risks associated with storing and accessing their data on remote servers. When users perceive a high level of vulnerability, they are more likely to take precautions and adopt security measures such as using strong passwords, enabling two-factor authentication, and regularly updating their devices and applications. On the other hand, if users perceive a low level of vulnerability, they may neglect these security measures, leaving their data vulnerable to unauthorized access or cyber-attacks. The level of perceived vulnerability can be influenced by various factors such as media reports on data breaches or personal experiences with security incidents. For example, if a user hears about a high-profile data breach involving mobile cloud computing services, they may perceive a higher level of vulnerability and take immediate action to enhance their security measures. Furthermore, the design and implementation of mobile cloud computing platforms also play a significant role in shaping users' perceptions of vulnerability. If service providers prioritize robust encryption protocols, regular security audits, and transparent privacy policies, users are more likely to have confidence in the platform's security features [21].

Individuals' perceptions regarding potential risks and threats influence their decision-making process. Higher education institutions are often reluctant to fully embrace this technology due to concerns about data security, privacy breaches, and unauthorized access to sensitive information. These concerns stem from the inherent nature of mobile cloud computing, where data is stored remotely on servers and accessed through various devices.

Students may perceive vulnerabilities such as data breaches, privacy concerns, and unauthorized access to their personal information. These perceived vulnerabilities can significantly impact their willingness to adopt this technology. Research has shown that students who perceive themselves as vulnerable are less likely to adopt mobile cloud computing in their academic pursuits [22]. They may fear that their personal information or academic work could be compromised or misused. This fear can hinder them from fully embracing the benefits of this technology. If students and educators believe that their data is vulnerable to attacks or breaches, they may be hesitant to fully embrace this technology for educational purposes [23].

Response efficacy refers to an individual's belief in their ability to effectively respond to a threat or danger. In the context of MCC, response efficacy refers to an individual's belief in their ability to effectively respond to potential security threats associated with MCC. In higher education environment, response efficacy involves students' confidence in their ability to protect their data and mitigate potential security breaches. When students perceive high response efficacy towards addressing security threats associated with MCC, they are more likely to adopt this technology. This is because they feel confident that they can take appropriate measures to safeguard their information and prevent unauthorized access. On the other hand, if students perceive low response efficacy, they may be hesitant to adopt MCC due to fears of compromising sensitive data. When students and educators have confidence in their ability to protect their data through various security measures, they are more likely to embrace these technologies for educational purposes [22], [24].

The response cost refers to the effort required to mitigate or respond to a particular threat. As stated by PMT, the cost of adopting the recommended reaction, or the amount of labor needed in performing the recommended response, has a major negative influence on adaptive behaviors. Actually, individuals are less likely to use the recommended response if they are inconvenienced or must expend a significant amount of effort, money, or time ([21], [25]). Scholars found that individuals" intentions to adopt adaptive activities are negatively influenced by response cost. Wu and Wang study the factors that influence user mobile commerce adoption; they argue that cost is a major inhibitor of behavioral intention to use mobile commerce, and that has a considerably negative direct effect on behavioral intention to use [26]. The same findings were corroborated by Reardon and Davidson, who investigated variables influencing poor adoption of health information technology such as electronic medical records and discovered that cost is one of the most significant impediments of behavioral intention to use electronic medical records ([15], [27]).

In context of MCC, response cost refers to the effort required to mitigate or recover from a security breach [28]. In the case of MCC adoption in higher education students, this includes implementing robust security measures such as encryption protocols, multi-factor authentication, and regular system updates. Additionally, educating students about safe online practices and raising awareness about potential risks are essential components of response cost. Students and educators may be deterred by the time-consuming process of securing their devices or recovering lost data if a breach occurs. The perceived high response cost can discourage them from utilizing mobile cloud computing for educational purposes. When students perceive that the response cost is high in relation to potential security threats associated with MCC, they may hesitate to adopt this technology fully. Concerns about unauthorized access to personal information or data breaches can deter them from utilizing MCC for academic purposes ([22], [29]). Thus, the following hypotheses are proposed:

H1: Perceived severity negatively influences students' intention to adopt MCC.

H2: Perceived vulnerability negatively influences students' intention to adopt MCC.

H3: Response efficacy positively influences students' intention to adopt MCC.

H4: Response cost negatively influences students' intention to adopt MCC.

2.4 User behavioral intention and Usage Behaviour

Behavioral intention refers to an individual's subjective likelihood or willingness to perform a specific behavior. Behavioral intention is regarded as a dominant factor in predicting the decision to perform a specific behavior for several information systems theories, such as the Theory of Planned Behavior Model (TPB), the Technology Acceptance Model (TAM), the Theory of Reasoned Action Model (TRA), and the Decomposed Theory of Planned Behavior Model (DTPB). All of these models have been successfully and widely used to predict and understand how actual behavior will behave in a variety of contexts and subject areas [30], [31], [32], [33], and [34], and they all support the fact that behavioral

intention has a significant direct impact on actual behavior [15]. This concept suggests that an individual's intention to engage in a particular behavior is a strong predictor of whether they will actually carry out that behavior. As with prior studies, this study predicts that when students intend to adopt MCC, they are more motivated to adopt it for educational purposes. Thus, the following hypothesis is proposed:

H7: Students' intention to adopt MCC for their educational purposes is positively related to their actual adoption of MCC on their mobile devices.

3. Methodology

3.1 Measurement

Defining the constructs that a study attempts to assess and choosing appropriate measurement techniques are crucial steps that have a significant impact on the accuracy of the study's results [35], [36]. In this study, the survey instrument was created by the researcher to test the research hypotheses. In order to guarantee the scale's face (content) validity; items from earlier studies were identified and utilized in the survey questionnaire to measure the constructs. The items were utilized frequently in the majority of prior studies showing a probable subjective consensus among scholars that these measuring instruments seem to accurately reflect the constructs of interest. The items created for each construct in this study are listed in Table 1, along with the previous studies from which they were adapted.

3.2 Data Collection Procedures

To achieve the study goals, the study's sample surveyed students of Shaqra and Imam Mohammad Ibn Saud Islamic universities. A fully completed survey was obtained from 403 students. After checking the data for validity, 372 of them were deemed fit for use.

In information systems research, an adequate sample size for undertaking partial least squares (PLS) path analysis is critical [39]. A typical information systems study would have at least 0.25 R-squared values, a 5% significance level, and 80% statistical power. A sample size of 59 is thought to be adequate when using such attributes with a maximum of three arrows pointing to a latent variable [40] as defined in the study's structural equation model (see Figure 1). However, with the aforementioned parameters and factor loadings of 0.5, the ideal sample size is 78 [39]. As a result, the sample size of 372 seemed to be more than adequate for this study.

Table 1: List of items by construct

Construct	Items	Adapted from
Perceived Severity (PS)	How strongly do you disagree or agree with the following statements? PS1. MCC applications pose a severe security risk to your mobile systems. PS2. MCC applications can transmit sensitive data to third parties (e.g., passwords, usernames, and customer information). PS3. MCC applications can allow remote access to your mobile. PS4. MCC applications can be used to download and install malicious applications.	[15], [37].
Perceived Vulnerability (PV)	How likely is MCC applications to affect your mobile in the following ways? PV1. Transmit sensitive data to third parties. PV2. Allow access to remote attackers. PV3. Install malicious applications.	[15], [18].

Response Efficacy (RE)	RE1. Installing anti-virus software will successfully prevent MCC attacks. RE2. Anti-virus software is the best solution for counteracting problems caused by MCC applications. RE3. If you install anti-virus software on your mobiles, you can minimize the threat of MCC applications.	[15], [18].
Response cost (RC)	RC1. Anti-virus software is expensive to purchase and operate. RC2. You have to upgrade your mobile's system to install anti-virus software. RC3. Anti-virus software can slow down your mobile's system.	[38], [26].
Behavioral intention (BI)	BI1. You intend to install and use MCC applications on your mobile's device in next three months. BI2. You expect that your use of the MCC applications to continue in the future.	[32], [30], [34].
MCC Usage (US)	US1. On average, each week you use MCC applications on your mobile's device often. US2. Every morning, you check your MCC applications.	[15], [30], [34].

1.

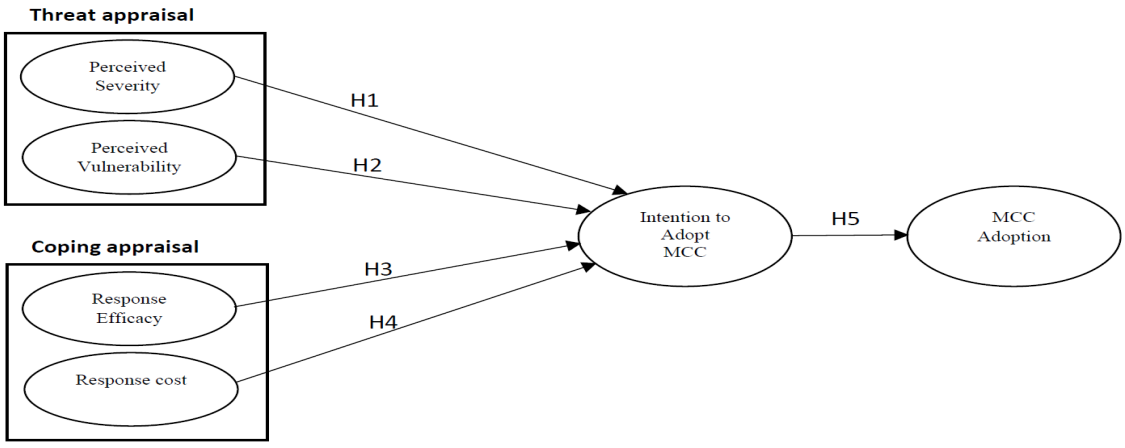

Fig. 1 The study model.

Table2: Cronbach's Alpha Reliability of Constructs

Construct	Number of Items	Cronbach's Alpha
Perceived Severity (PS)	4	.985
Perceived Vulnerability (PV)	3	.973
Response Efficacy (RE)	3	.957

Response cost (RC)	3	.942
Behavioral intention (BI)	2	.972
MCC Usage (US)	2	.955
Overall alpha value	24	.964

Table 3: Factor Analysis of Items Sorted by Construct (Rotated Component Matrix (a))

	Component					
	1	2	3	4	5	**Its assessment**
PS1	**.819**	.356	.297	.142	-.138	*Excellent > 0.71*
PS2	**.787**	.454	.376	.179	.075	*Excellent > 0.71*
PS3	**.781**	.470	.369	.067	.072	*Excellent > 0.71*
PS4	**.791**	.465	.364	.069	.066	*Excellent > 0.71*
PV1	.357	**.857**	.189	.129	-.149	*Excellent > 0.71*
PV2	.463	**.793**	.243	.175	-.035	*Excellent > 0.71*
PV3	.469	**.803**	.249	-.039	-.111	*Excellent > 0.71*
RE1	.503	**.772**	.371	.092	.231	*Excellent > 0.71*
RE2	.557	**.662**	.329	.094	.291	*Very good > 0.63*
RE3	.579	**.696**	.349	-.017	.233	*Very good > 0.63*
RC1	**.748**	.592	.329	.071	-.048	*Excellent > 0.71*
RC2	**.773**	.512	.353	.033	.019	*Excellent > 0.71*
RC3	**.791**	.501	.357	.043	.037	*Excellent > 0.71*
BI1	**.764**	.495	.367	.024	.020	*Excellent > 0.71*
BI2	**.739**	.474	.391	.121	.062	*Excellent > 0.71*
US1	**.642**	.514	.365	.473	.026	*Very good > 0.63*
US2	**.720**	.366	.378	.317	.046	*Excellent > 0.71*

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 6 iterations

4. Data analysis and Results

4.1 Reliability and validity

The instrument's internal consistency and reliability have been tested using the collected data from the pilot study of each construct in the instrument. The findings indicate that alpha values ranged from.942 to.985, with a mean of.964 (see Table 2). This implies that each construct in the model was reliable. The internal consistency was therefore adequate.

Construct validity was determined by evaluating a principal component analysis with a varimax rotation using factor analysis. The convergent and discriminant validity of items were estimated using this method. Convergent validity was tested by determining whether or not items from a variable converged on a single construct [41] and whether the factor loading for each item was greater than 0.45, as recommended by Comrey & Lee [42]. Loadings greater than 0.45 could be considered fair, while loadings greater than 0.55 could be considered good, 0.63

very good, and 0.71 excellent, according to Comrey and Lee [42]. The discriminant validity was determined by examining the cross-loading of items on various factors. Table 3 shows that there is no evidence of weak loading.

4.2 Hypotheses testing

This study investigates the determinants of the educational use of mobile cloud computing among students.

Assuming that the decision of students to adopt MCC applications is strongly influenced by both threat and coping appraisals, this study proposes and develops a theoretical model by adopting and modifying PMT (see Figure 1).

As indicated in Figure 1, the study's model is constructed by testing five formulated hypotheses. These hypotheses establish the relationship between components as independent variables that impact MCC adoption behaviour. For dependent variables, each accepted hypothesis offers an explanation of usage behaviour. Explanations are nomothetic and progress through deductive reasoning. Pearson's correlation analysis was used to perform a simple correlation among all of the research variables, as shown in Table 4. We used the regression model to examine multicollinearity by analysing collinearity statistics, such as the Variance Inflation Factor (VIF) and tolerance, since variables exhibited significant correlations (p0.01).

To find out if there were any multicollinearity impacts, we looked for any warning messages given by the AMOS output that indicated a multicollinearity concern. There was no indication of multicollinearity in the results. The potential problem of multicollinearity can be investigated explicitly in the context of regression analysis.

Tolerance values in Table 5 varied from 0.413 to 0.424. The use of variance inflation factors (VIF) is one method for measuring collinearity. Although a variance inflation factor (VIF) of less than or equal to 10 (i.e. tolerance >0.1) is typically recommended ([43], [44]). A variance inflation factor (VIF) larger than 4 is regarded to be a major problem of multicollinearity in this study. However, as shown in Table 6, there were no VIF values greater than 4 in the model, since the VIF values varied from 2.319 to 2.912. As a result, there was no indication of multicollinearity.

Table4: Correlation analysis amongst the variables

	US	BI	RC	RE	PV
BI	.887*				
RC	.716*	.725*			
RE	-.819*	-.867*	-.751*		
PV	.836*	.878*	.762*	-.960*	
PS	.829*	.889*	.728*	-.974*	.947*

US: Usage, BI: Behavioral intention, RC: Response cost, RE: Response Efficacy, PV: Perceived Vulnerability, PS: Perceived Severity. * $p \leq 0.01$

Table5: Multicollinearity test

Dependent variable	Path direction	Independent variables (predictors)	Collinearity Statistics	
			Tolerance	VIF
Usage	←	Intention	.424	2.357
Intention	←	Perceived Severity	.413	2.419
Intention	←	Perceived Vulnerability	.421	2.355
Intention	←	Response Efficacy	.423	2.319
Intention	←	Response cost	.416	2.912

The study hypotheses are evaluated using multiple regression analysis after ensuring that all relevant requirements are satisfied. First, "Intention" was regressed on "Usage". As shown in Fig. 2, "Intention" (β=0.887, Standardized path coefficient, $p < 0.05$) is shown to be substantially and positively associated to "Usage" (adjusted R^2=0.786) (see Tables 6, 7, and Fig. 2). As a result, H5 is supported.

Thereafter, the four independent variables (i.e. “Perceived Severity”, “Perceived Vulnerability”, “Response Efficacy”, and “Response cost”) were regressed on “Behavioral Intention”. Results, as in Fig. 2, indicate that all four variables are significantly related to “Behavioral Intention” (adjusted R^2=0.812): “Perceived Severity” (β = 0.776, Standardized path coefficient, $p < 0.05$), “Perceived Vulnerability” (β = 0.386, Standardized path coefficient, $p < 0.05$) , “Response Efficacy” (β = -0.363, Standardized path coefficient, $p < 0.05$) and “Response cost” (β = -0.138, Standardized path coefficient, $p < 0.05$) (see Table 6, Table 7 and Fig. 2). Thus, H1, H2, H3 and H4 are supported.

Table6: Coefficients for Proposed model

Dependent variable	Path direction	Independent variables (predictors)	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
			B	Std. Error	Beta		
Usage	←	Intention	.839	.023	.887	36.980	.000
Intention	←	Perceived Severity	.849	.110	.776	7.721	.000
Intention	←	Perceived Vulnerability	.397	.087	.386	4.575	.000
Intention	←	Response Efficacy	-.380	.112	-.363	-3.115	.000
Intention	←	Response cost	.151	.038	.138	3.954	.000

P values less than 0.05 were considered statistically significant

Table7: Standardized Regression Weights

Criterion variable	Path direction	Criterion variable predictors	Estimate	(Significance)
Usage	←	Intention	.887	Significant
Intention	←	Perceived Severity (PS)	.776	Significant
Intention	←	Perceived Vulnerability (PV)	.386	Significant
Intention	←	Response Efficacy (RE)	-.363	Significant
Intention	←	Response cost (RC)	.138	Significant

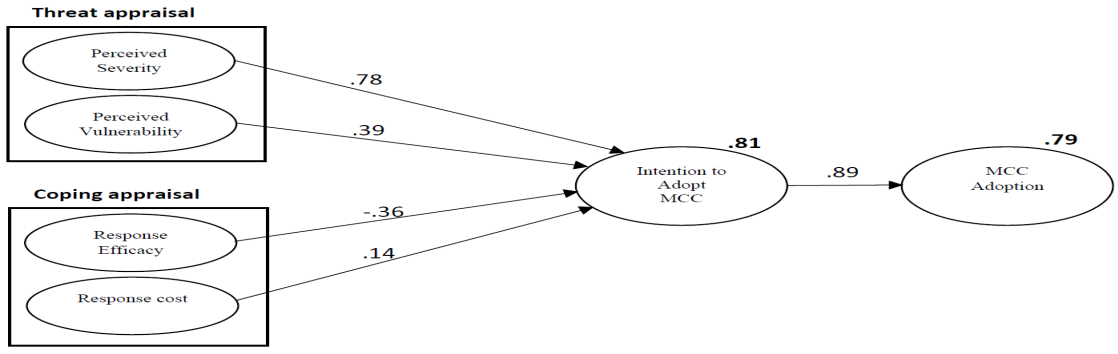

Fig. 2 The study model.

5. Discussion

This study proposes and develops a theoretical model by adopting and modifying PMT. The study model investigate the determinants of the educational use of mobile cloud computing in higher education. The study's findings show that a significant amount of variance in MCC adoption was explained by the proposed model. All of the study's hypotheses are supported. MCC adoption intention was shown to be highly influenced by threat appraisal and coping appraisal factors.

This suggests that student's decision regarding the MCC adoption is effected by both the level of negative consequences from using MCC application and mobile's systems vulnerability to the attacks, as well as magnitude of beliefs regarding whether the installing and using anti-virus software, as a recommended preventive response, will be effective in avoiding or reducing security threat.

In an earlier study, the author developed an equation to approximate the contribution of each model's construct to the model's explanatory power [45].

$$A_x = \frac{\beta_x{}^2}{\sum_{k=1}^{n} \beta_x{}^2} \times R_{PC}{}^2$$

Where:

A_x = Participation of variable A_x in a model' explanatory power

$\beta_x{}^2$= Square of beta coefficients or standardized coefficients of variable

$R_{PC}{}^2$= Model' explanatory power

$\sum_{k=1}^{n} \beta_x{}^2$= Total of causal effects for the model's constructs

The study applies the equation mentioned above to calculate the explanatory power of every construct and its antecedents, as well as the rate at which each antecedent adds to a construct's explanatory power. The formula was used to calculate how much the "intention's" antecedents contributed to its explanatory power. Table 8 summarizes the findings.

The findings demonstrate that university students' intention toward using mobile cloud computing are significantly influenced by Perceived Severity, Perceived Vulnerability, Response Efficacy and Response cost, which have the ability to explain their intention to use MCC by 37.80%, 18.80%, 17.68% and 6.72% respectively.

Table8: Participation of Intention's variables in its explanatory power

Antecedents	Intention
Perceived Severity	37.80%
Response cost	18.80%
Perceived Vulnerability	17.68%
Response Efficacy	6.72%
Total	81.00%

As aforementioned, perceived severity alone explains 37.8% of students "Intention" to adopt MCC applications, which indicates the student's perception of the degree of harm that would happen can hinder them from using MCC. It encompasses concerns about data security, privacy breaches, and academic integrity issues. The study findings indicate that perceived severity was the most influential factor in determining students' intentions to adopt these applications.

The high percentage explained by perceived severity underscores its significance in shaping students' decision-making process. Students are becoming increasingly aware of the potential risks associated with using MCC applications and are more cautious when considering their adoption. This finding highlights the need for technology developers and educators to prioritize addressing these concerns through robust security measures and comprehensive user education.

While other factors may also contribute to students' intention to adopt MCC applications, such as response cost, perceived vulnerability, and response efficacy, perceived severity emerges as a dominant factor in this study. It suggests that efforts should be directed towards minimizing potential harm and ensuring a secure environment for

student users. This finding is consistent with Lee and Larsen's study, which found that perceived severity was the most influential factor, showing that the degree of expected harm from malware attacks is the strongest motivator of software adoption [25].

"Response cost", "Perceived vulnerability," and "Response Efficacy" also have significant influence on students "intention" to adopt MCC applications by 18.8%, 17.7%, and 6.7%, respectively.

In the context of this study, response cost refers to the potential negative consequences or costs that students may face when adopting the MCC application. As stated above, the study findings show that "Response cost" has the ability to lessen the "intention" of students to adopt MCC by 18.8%. When considering the adoption of MCC applications, students are likely to weigh the potential benefits against the perceived costs. The study found that response cost accounts for a significant portion of students' intention to adopt MCC applications. This suggests that students are aware of the potential negative consequences and consider them in their decision-making process.

One possible explanation for this finding is that students may be concerned about the time and effort required to solve the problems that might arise when they use MCC applications. They may fear that using these applications will be time-consuming and take away from other important tasks or activities. Additionally, they may worry about technical difficulties or compatibility issues with their devices.

Another factor contributing to response cost could be financial concerns. Students may perceive the security and privacy issues that might arise when they use MCC applications as expensive or requiring additional expenses such as data plans or device upgrades. This financial burden could deter them from adopting these applications.

This result is consistent with the majority of earlier research in other contexts of the information systems adoption literature, such as the Wu and Wang study, which argues that cost is one of the most important inhibitors of behavioral intention to use mobile commerce and that this has a significantly negative impact on behavioral intention to use [26]. The same findings were corroborated by Reardon and Davidson, who investigated the factors influencing a lack of acceptance of health information technology such as electronic medical records and discovered that cost is one of the most significant obstacles to behavioral intention to use electronic medical records [27].

The adoption of Mobile Cloud Computing has become increasingly prevalent among students. However, with this technological advancement comes concerns about the vulnerability of their devices to virus or malware attacks. Perceived vulnerability refers to the notion that individuals believe their devices are at risk of being exploited by such malicious attacks. Students are expected to seriously consider this perceived vulnerability before embracing MCC. While MCC offers numerous benefits, including increased accessibility and storage capacity, it also poses potential risks. With cloud-based services, students store their data on remote servers rather than locally on their devices. This shift in data storage raises concerns about unauthorized access and cyber threats.

The influence of perceived vulnerability was relatively weaker than expected, but it still has a significant effect on the intention" of students to adopt MCC applications. The result means that students are expected to seriously consider whether the adoption of MCC makes their devices vulnerable to a high probability of being exploited by virus or malware attacks. This finding is consistent with most prior studies that have shown that when a person perceives high vulnerability, the probability of adopting protective behaviors is increased, which means that perceived vulnerability has a significant effect on their intentions to adopt protective behaviors [17], [25].

To mitigate these risks, students must take proactive measures to protect their devices from virus or malware attacks. This includes regularly updating antivirus software, using strong passwords for cloud accounts, and being cautious when downloading files or clicking on suspicious links. Moreover, educational institutions should also play a role in ensuring the security of student devices by implementing robust cybersecurity measures. This can involve providing comprehensive training on safe internet practices and offering technical support for any security-related issues.

Response efficacy also has strong impact on adoption intention, with its 6.72% ability to explain students' intention to adopt MCC. In the context of this study, response efficacy refers to the ability of students to effectively address and resolve issues that arise when they adopt Mobile Cloud Computing technology, which may make their devices vulnerable to virus or malware attacks. In today's digital age, where technology plays a pivotal role in education, it is crucial for students to possess the necessary skills and knowledge to navigate potential risks. When students embrace MCC, they gain access to a wealth of resources and collaborative tools that enhance their learning experience. However, this convenience comes

with inherent risks. The interconnectedness of devices through cloud computing exposes them to various cyber threats. Viruses and malware can infiltrate devices, compromising personal information and disrupting the learning process.

The results show that students are highly motivated to use anti-virus software when the expected returns from using the suggested protection measures are high. Anti-virus software has been found to be an effective and efficient solution for detecting and preventing virus threats; thus, it is expected that installing anti-virus software will provide mobile users confidence that this solution will prevent or reduce the security danger. These findings are consistent with the findings of LaRose et al., [23] and Johnston and Warkentin [6], who discovered that both response efficacy and self-efficacy had a substantial influence on intentions to engage in protective actions. LaRose et al. [23] showed that self-efficacy and response efficacy were the most related to intentions to engage in secure activities on the internet [23]. In their study, Johnston and Warkentin examine the effect of fear appeals on end-user compliance with suggestions to take particular individual computer security activities to mitigate dangers. According to the findings, self-efficacy and response efficacy impact end-user behavioral intentions [6].To ensure response efficacy, students must be equipped with the necessary skills to identify and mitigate these risks. Educational institutions should prioritize cybersecurity education as part of their curriculum. By teaching students about safe browsing habits, recognizing phishing attempts, and implementing effective security measures such as antivirus software and regular updates, they can develop resilience against potential attacks.

Moreover, fostering a culture of responsibility is essential in promoting response efficacy. Students should be encouraged to report any suspicious activities or incidents promptly so that appropriate actions can be taken. Collaboration between educational institutions, parents/guardians, and technology providers is vital in creating a secure environment for students.

References

[1] CISCO. “Mobility: Transforming the Internet for the future,” In *CISCO Reports.* Retrieved January 9, 2023, from https://www.cisco.com/c/dam/en/us/solutions/collateral/executive-perspectives/annual-internet-report/air-executive-summary-pgr-mobility.pdf

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches,” *Wireless Communications and Mobile Computing,* vol. 13, no. 18, pp. 1587–1611, 2013.

[3] M. Almaiah and A. Al-Khasawneh, "Investigating the main determinants of mobile cloud computing adoption in university campus," *Education and Information Technologies*, vol. 25, pp. 3087-3107, 2020.

[4] W. Al-Ghaith, "Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices,” *International Journal of Computers,* vol. 10, pp. 125-138, 2016.

[5] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983-988, 2012.

[6] R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse," MIS Quarterly, vol. 37, no. 1, pp. 1-20, 2013.

[7] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183-196, 2010.

[8] M. Maray and J. Shuja, "Computation offloading in mobile cloud computing and mobile edge computing: survey, taxonomy, and open issues." *Mobile Information Systems,* 2022.

[9] J. Wan, C. Zou, S. Ullah, C. Lai, M. Zhou and X. Wang, “Cloud-enabled wireless body area networks for pervasive healthcare,” *IEEE Network,* vol. 27, no. 5. pp.56-61, 2013.

[10] X. Jin, W. Hua, Z. Wang and Y. Chen, “A survey of research on computation offloading in mobile cloud computing,” *Wireless Networks,* vol. 28, no. 4, pp.1563-1585, 2022.

[11] M. I. Sahu and U. Pandey, ``Mobile cloud computing: Issues and challenges," in Proc. Int. Conf. Adv. *Comput., Commun. Control Netw. (ICAC-CCN),* Oct. 2018, pp. 247_250.

[12] A.S. Al-Ahmad, H. Kahtan, F. Hujainah and H.A. Jalab, “Systematic literature review on penetration testing for mobile cloud computing applications,” *IEEE Access,* VOL. 7, pp. 173524-173540, 2019.

[13] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal Of Psychology,* vol. 91, no. 1, pp. 93-114, 1975.

[14] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in *Social Psychophysiology*, New York, Guilford Press, 1983, p. 153–176.

[15] W. Al-Ghaith, “Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices,”

International Journal of Computers, vol. 10, pp. 125-138, 2016.

[16] S. Milne, P. Sheeran and S. Orbell, "Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory," *Journal of Applied Social Psychology,* vol. 30, no. 1, p. 106–143, 2000.

[17] B. T. McClendon and S. Prentice-Dunn, "Reducing skin cancer risk: an intervention based on protection motivation theory," *Journal of Health Psychology,* vol. 6, p. 321–328, 2001.

[18] C. Pechimann, G. Zhao, M. E. Goldberg and E. T. Reibling, "What to convey in antismoking advertisements for adolescents: the use of protection motivation theory to identify effective message theme," *Journal of Marketing,* vol. 67, no. April, p. 1–18, 2003.

[19] H. M. Alnajrani and A. A. Norman, "The effects of applying privacy by design to preserve privacy and personal data protection in mobile cloud computing: An exploratory study," *Symmetry,* vol. 12, pp. 2039, 2020.

[20] H. R. Nikkhah, V. Grover and R. Sabherwal, "Post hoc security and privacy concerns in mobile apps: the moderating roles of mobile apps' features and providers," *Information & Computer Security*, vol. ahead-of-print, no. ahead-of-print, 2023.

[21] R. Palanisamy and Y. Shi, "Users' attitude on perceived security of mobile cloud computing: empirical evidence from SME users in China," Information & Computer Security, vol. 31, no. 1, pp. 65-87, 2023.

[22] M. Al-Emran, M. N. Al-Nuaimi, I. Arpaci, M. A. , Al-Sharafi and B. Anthony Jnr, "Towards a wearable education: Understanding the determinants affecting students' adoption of wearable technologies using machine learning algorithms," *Education and Information Technologies,* vol. 28, no. 3, pp. 2727-2746, 2023.

[23] H. Al-Samarraie and N. Saeed, "A systematic review of cloud computing tools for collaborative learning: Opportunities and challenges to the blended-learning environment," *Computers & Education,* vol. 124, pp. 77-91, 2018.

[24] K. Kumar, D. Liu and L. Carter, "Understanding the adoption of digital conferencing tools: Unpacking the impact of privacy concerns and incident response efficacy," *Computers & Security*, vol.132, pp. 103375, 2023.

[25] Y. Lee and K. R. Larsen, "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software," *European Journal of Information Systems,* vol. 18, pp. 177-187, 2009.

[26] J. H. Wu and S. C. Wang, "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Information & Management,* vol. 42, no. 5, p. 719–729, 2005.

[27] J. L. Reardon and E. Davidson, "An organizational learning perspective on the assimilation of electronic medical records among small physician practices.," *European Journal of Information Systems,* vol. 16, no. 6, pp. 681-694, 2007.

[28] D. Marikyan, S. Papagiannidis, O. F. Rana and R. Ranjan, "Blockchain adoption: A study of cognitive factors underpinning decision making," *Computers in Human Behavior,* vol. 131, pp. 107207, 2022.

[29] M. Al-Emran, A. Granić, M. A. Al-Sharafi, N. Ameen and M. Sarrab, "Examining the roles of students' beliefs and security concerns for using smartwatches in higher education," *Journal of Enterprise Information Management*, vol. 34, no. 4, pp. 1229-1251, 2021.

[30] W. Al-Ghaith, "Understanding Social Network Usage: Impact of Co-Presence, Intimacy, and Immediacy," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 6, no. 8, pp. 99-111, 2015.

[31] B. Sheppard, J. Hartwick and P. Warshaw, "The theory of reasoned action: a meta-analysis of past research with recommendations for modifications and future research," *Journal of Consumer Research,* vol. 15, no. 3, p. 325–343, 1988.

[32] S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," *Information Systems Research,* vol. 6, no. 2, pp. 144-176, 1995.

[33] L. Chen, L. M. Gillenson and L. D. Sherrell, "Consumer acceptance of virtual stores: a theoretical model and critical success factors for virtual stores," *ACM SIGMIS Database,* vol. 35, no. 2, pp. 8-31, 2004.

[34] W. Al-Ghaith, "Using the Theory of Planned Behavior to Determine the Social Network Usage Behavior in Saudi Arabia," *International Journal of Research in Computer Science,* vol. 5, no. 1, pp. 1-8, 2015.

[35] E. Bell, A. Bryman and B. Harley, Business research methods. Oxford university press, 2022.

[36] W. G. Zikmund, Business research methods (7th ed.), Cincinnati, OH: Thomson, 2003.

[37] I. M. Y. Woon, G. W. Tan and R. T. Low, "A protection motivation theory approach to home wireless security," in *The Twenty-Sixth International Conference on Information Systems (Avison, D., Galletta, D., & DeGross, J., Eds)*, Las Vegas, 2005.

[38] V. Venkatesh, M. Morris, M. G. Rris, G. B. Davis and F. D. Davis, "User acceptance of information technology: toward a unified view," *MIS Quarterly,* vol. 27, no. 3, p. 425–478, 2003.

[39] G. A. Marcoulides and C. Saunders, "Editor's comments: PLS: a silver bullet?," *MIS quarterly,* pp. iii-ix, 2006.

[40] K. K. K. Wong, "Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS," *Marketing Bulletin,* vol. 24, no. 1, pp. 1-32, 2013.

[41] G. Premkumar and K. Ramamurthy, "The role of Interorganizational and organizational factors of the decision mode for adoption of interorganizational systems," *Decision Science,* vol. 26, no. 3, pp. 303-336, 1995.

[42] A. L. Comrey and H. B. Lee, A first course in factor analysis, L., NJ: Erlbaum Associates, 1992.

[43] H. B. Asher, Causal modeling, Newbury Park: Sage University Press, 1983.

[44] M. Lee, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," *Electronic Commerce Research and Applications,* vol. 8, no. 3, pp. 130-141, 2009.

[45] W. Al-Ghaith, "Understanding Social Network Usage: Impact of Co-Presence, Intimacy, and Immediacy," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 6, no. 8, pp. 99-111, 2015.

Waleed Alghaith is an associate professor at Al Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. He was appointed as a Vice Dean and then Dean of information Technology Deanship and E-learning Deanship. He was then appointed as a Vice Dean of the Institute of Research and Studies and Secretary General of the Scientific Council. He was appointed also as a Head of Information Systems Department. His current research interests are in Cloud Computing, Sentiment Analysis, enterprise information systems, machine learning, Artificial Intelligence, Technology Adoption, Cyber Security.