Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

The Factors Influencing the Use of Password Managers

Hussain Alshahrani*, and Abdulrahman Alghamdi
Department of Computer Sciences, College of Computing and Information Technology, Shaqra University, Sahqra, Saudi Arabia.

Received 01 Apr. 2022; Accepted 20 June. 2022; Available Online 25 June. 2022

Abstract

This paper investigates the factors that influence the actual use of password managers. In this paper, we have integrated some factors from the Technology Acceptance Model (perceived ease of use, perceived usefulness, and attitude) with other factors from the literature review (user readiness, awareness, and motivation) to investigate the influence of these factors on the use of password managers. The authors used an online questionnaire to collect data. The questionnaire was distributed by using two social media platforms (Twitter and WhatsApp). There were 171 participants from 6 countries who completed the questionnaire. Structural equation modelling was employed by using SmartPLS-3 software to analyse the data. Findings indicate that perceived ease of use, perceived usefulness, and user readiness have a positive impact and are substantially associated with attitude, thus influencing the actual use of password managers. Likewise, perceived usefulness, user readiness, and awareness have a positive impact and are significantly associated with motivation of users to use it, which also influences the actual use of password managers.

I. Introduction

In the last decade, the use of new technologies has dramatically increased. A large number of literature reviews show and provide evidence for this use [17, 23, 28,31,35,37]. Among these technologies, there is one that has been developed to help users keep and remember the passwords of their accounts and online profiles. This technology is called password managers. It is an encrypted digital vault that can store passwords securely [7]. Nowadays, the user has multiple passwords for different accounts, which makes it impossible to remember them [34,8]. Thus, the password manager can help the user to use different passwords for all the accounts without needing to memorize them.

There are different types of password managers. Colby and Hodge [7] and Turner [32] identified the best password managers; they include Zoho Vault, AgileBits 1Password, Dashlane, keeper password manager and digital vault, RoboForm 8 Every Where, Password Boss, LogMeOnce Password, Sticky Password Premium, Lastpass Premium, and Chrome. However, Colby and Hodge [46] have identified the best password manager to use for 2022, which includes the previous list and in addition to it Bitwarden. Despite the importance of this technology, however, the studies that pay attention to it are limited, so it needs more investigation. Ac-

Keywords: Cybersecurity, Password Managers, Technology Acceptance Model, Perceived Ease of Use, Perceived Usefulness, Attitude, User Readiness.

Production and hosting by NAUSS

* Corresponding Author: Hussain Alshahrani
Email: halshahrani@su.edu.sa
doi: 10.26735/TNJT2900

cording to [12], “Password managers, though commonly recommended by security experts, are still not used by many users.” According to a review of previous studies, they mainly focus either on factors affecting the adoption of password managers or focus on how this technology can be used. Therefore, the current study aims to investigate the factors that may encourage people to use password managers. The remainder of the paper is organized as follows: First, a relevant literature review is provided. Next, the methodology used in the study is explained. Then the findings of the study are presented. Finally, the paper concludes with a discussion of the findings and future research directions.

II. Literature Review

The use of new technology has received considerable attention from researchers and scholars. This attention is clearly seen from the large body of literature that has investigated this topic. Reviews of this literature have focused on the factors that affect the use or intention to use a new technology. For instance, Teo et al. [31] studied the intention to use technology among pre-service teachers in two contexts, Singapore and Malaysia. They employed the technology acceptance model (TAM) to conduct their study. In another study, Nikou and Economides [23] investigated the factors that influence behavioural intention to use mobile-based assessment.

A. Password Managers

Nowadays, there is a technology called password managers that is used to help users keep their passwords. According to [7], “A password manager is essentially an encrypted digital vault that stores secure password login information you use to access apps and accounts on your mobile device, websites and other services. In addition to keeping your identity, credentials and sensitive data safe, the best password manager also has a password generator to create strong, unique passwords and ensure you aren't using the same password in multiple places”. It might be argued that the password is still the key to keeping sensitive data secure on the internet [21]. Managing all the different passwords (including remembering them) is still a big problem [34], especially for private end-users who are sometimes quite careless with their passwords [13].

B. The Use of Password Managers

It must be stated that there are some negative actions that can be performed by end-users, such as frequent use of the same password for online accounts [29]. Survey results show that up to two-thirds of people use one password for multiple or all online profiles [8]. The standard user has thousands of personal and work-related passwords and finds it impossible to remember multiple passwords [8]. Also, cognitive demands increase as people use more devices, resulting in weaker password choices to handle the load. Login policies or suggestions on how to choose strong passwords do not help people remember passwords. Encouragement of password use does not mitigate the challenge of juggling multiple passwords and accounts. Password managers are one suggested solution to these password issues. Password manager applications are highly recommended to help users maintain passwords properly [29]. Password manager apps store all a user's passwords in an encrypted location and are accessible via an (ideally) strong master passcode, which reduces the pressure of keeping multiple strong individual passwords [29].

Studies of people's daily login practices and responsibilities [16,30] provide an essential basis for identifying user preference in password management. The standard user has approximately 16 to 26 password-protected user accounts [13], and recent estimates show that the regular user with a password manager at work may have hundreds of user accounts [18]. The reuse of passwords will seriously impact users and organizations affected by data breaches [6]. Experts, therefore, encourage the use of memorable, strong passwords with all platforms [20] or at least for company services [33]. It is also difficult for users to remember passwords, especially rarely used passwords, website passwords, and randomly produced passwords [36]. Alkaldi and Renaud [1] studied the reasons that can lead to adoption or rejection of smartphone password managers. In another study, Aurigemma et al. [4] argued that the lack of password manager usage might be due to lack of trust, perceived

costs and benefits, and lack of concern over the threat. Furthermore, Pearman *et al*. [27] interviewed 30 participants to find out why password managers were not used effectively. They found that the reasons were related either to convenience or to security. Fagan *et al*. [12] argued that convenience and usefulness are considered the main reasons for using password managers.

Some studies in the literature review have focused on the security and trust issues on password managers [42, 43, 44, 45]. Ray et al. [45] investigated why older people do not use password managers. In their study, they found that these people have a mistrust of cloud storge of password managers. Also, older adults are concerned about the risks of a single point of failure. Moreover, Ray et al. discussed some of the possible adoption motivators that may encourage those people to adopt it. They have argued that these older people may have adopted password managers because of the recommendations of their families. They also argued that education may play a role to provide familiarity to password managers. Chaudhary et al. [44] conducted a systematic review to investigate the usability, security, and trustworthiness of password managers. In another study, [43] studied the relationship of initial trust and the intention to adopt password managers.

There are some challenges that might face the use of password managers. However, this issue still needs more investigation. According to a review of previous studies, they mainly focus either on factors affecting the adoption of password managers or focus on how this technology can be used. Based on the researchers' knowledge, there is no study focusing on the factors that influence the actual use of password managers.

C. The Types of Password Managers Used

There are several types of password managers that can be used. These types are classified based on stand-alone applications and built-in applications. Table I summarizes some of the most common password managers. Most stand-alone password managers are frequently offered as browser plugins (e.g., LastPass). Password managers keep passwords in three ways: locally (e.g., Keepass), cloud/web-based (e.g., LastPass), or without storage or hashing (e.g., LastPass and PwdHash) [32].

III. Research Model and Hypotheses

Fig. 1 illustrates the research model used to examine the factors that influence the use of password managers. These factors include perceived ease of use, perceived usefulness, user readiness, awareness, attitude, and motivation to use.

A. Perceived Ease of Use

Perceived ease of use is one of the important concepts of TAM; it is defined as the degree to which a person believes that he or she can use a new technology easily and without effort [10]. Our research defines it as the extent to which the user believes that the use of password managers is easy and effortless.

There is a large body of research which found that perceived ease of use significantly affects attitudes towards using technology [17, 28, 31, 35, 37, 23]. In line with previous studies, the following hypothesis can be proposed.

H1: Perceived ease of use (PEOU) has a significant influence on attitude towards use of password managers

B. Perceived Usefulness

Perceived usefulness, another important concept of TAM, is defined as the degree to which the user believes that the use of a new technology can be beneficial for him or her [10]. Thus, this paper can define perceived usefulness as the extent to which the users believe that the use of password managers can benefit them by keeping their passwords.

There are several studies that have found a significant relationship between perceived usefulness and attitude [17, 28, 31, 35, 37, 23], and between perceived usefulness and motivation [41]. According to these previous studies, the following two hypotheses can be proposed:

H2: Perceived usefulness (PU) has a significant influence on attitude towards use of password managers.

H3: Perceived usefulness (PU) has a significant influence on motivation to use password managers.

TABLE I
THE COMMON PASSWORD MANAGERS APPLICATIONS

Categories	Stand-Alone Applications									Built-in Applications
Evaluation Criteria	**Zoha Vault**	**AgileBits 1Password**	**Dashlane**	**keeper password manager and digital vault**	**RoboForm 8 Every Where**	**Password Boss**	**LogMeOne Password**	**Sticky Password Premium**	**Lastpass Premium**	**Chrome**
Generate automatic password	√	√	√	√	√	√	√	√	√	√
Verifies that the site is not an imposer	√	√	√	√	√	√	√	√	√	√
Identified reuse password	√	√	√	√	√	√	√	√	√	x
Blinded to customer support	√	√	√	√	√	√	√	√	√	x
Recovery via a physical object	x	x	√	x	x	x	x	x	x	√
Recovery via trustee	√	x	x	√	√	√	√	√	√	x
Published security architecture	√	x	√	√	√	√	√	√	√	x
authentication factor Multi	√	√	√	√	√	√	√	√	√	√

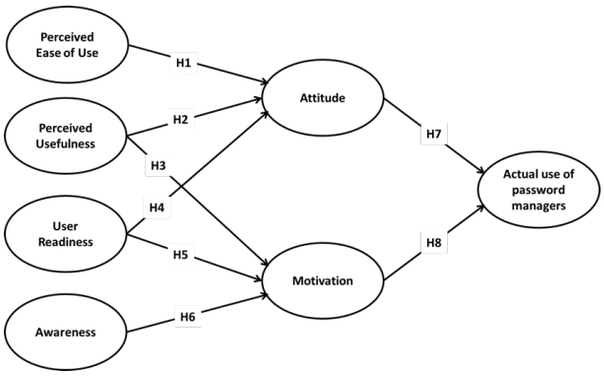

Fig. 1 Research Model.

C. User Readiness

There are many studies that have defined readiness for using new technologies. For example, Parasuraman and Colby [26] have defined readiness for technology as "people's propensity to embrace and to use new technologies for accomplishing goals in home life at the workplace" (p. 48). Thus, the current study defines user readiness for using password managers as the extent to which the user is ready and able to use password managers.

There are many studies that have investigated readiness for using new technologies [26, 22, 24]. The use of a new technology is based on the readiness of the users themselves [22]. Ling and Moi [22] have studied students' technology readiness for an e-learning system. Cheon et al. [5] argued that the use of mobile learning is based on the students' readiness for its use. Likewise, [24] have investigated the effect of technology readiness on a mandatory web-based system. According to these studies, the following two hypotheses can be proposed:

H4: User Readiness (UR) has a significant influence on attitudes towards use of password managers.

H5: User Readiness (UR) has a significant influence on motivation to use password managers.

D. Awareness

Awareness is the ability of the users to know how, why, and when they use password managers. Selevicence and Burkaitieve [38] investigated students' awareness in using Web2.0 tools for learning English. They found that awareness was an important factor in students' use of these tools to learn English. Likewise, Asiksoy [3] argued that the awareness of students and pre-service teachers in using Web2.0 for learning a foreign language was very important. Therefore, it can be hypothesized that:

H6: Awareness (AW) has a significant influence on motivation to use password managers.

E. Attitude

Attitude is defined as the degree to which persons are interested in using a new technology [40]. For purposes of the current research, attitude is the degree to which the user is interested in using password managers to keep his or her passwords.

The importance of attitude and its effect on the intention to use, or actual use of, a new technology has been shown by many scholars [28, 35]. Thus, the following hypothesis can be proposed:

H7: Attitude (AT) towards using password managers has a significant influence on their actual use

F. Motivation

According to [9], "Motivation is comprised of internal and external components of human life that encourage or discourage behaviours". Thus, motivation can be defined as the internal and external factors that encourage individuals to use password managers. Motivation to use a new technology is considered one of the important factors. Cullen and Greene [9] studied teachers' motivation to engage in technology integration activities. They found that motivation has a significant influence on the integration of the technology. Thus, the following hypothesis can be proposed:

H8: Motivation to use (MU) password managers has a significant influence on their actual use.

G. Actual Use of Password Managers

There are many factors that can influence the use of new technologies. Amongst these factors, perceived ease of use, perceived usefulness, and attitude are considered the most important in terms of impact on usage. In fact, these factors are regarded as the main components of TAM [10]. This model has been used effectively by a large number of studies to investigate the factors that influence the use of new technologies [17,28,31,35,37,23]. Thus, the current study has used this model to investigate how these factors can influence the use of password managers.

Several studies have found that user readiness [5], awareness [3], and motivation to use [9] are important factors affecting the use of new technologies. Therefore, this study has adopted and integrated these factors with the three components of TAM (perceived ease of use, perceived usefulness, and attitude) to investigate the factors that influence the use of password managers.

VI. Methodology

An online questionnaire is considered the most effective approach with which to gather data from a large number of people and from one or more locations [11, 2]. Therefore, this method was chosen to collect data for the present study. The items in the questionnaire are adopted from previous studies which investigated the factors that affect the use of a new technology.

Table II summarizes the sources of these items to measure the key variables in the questionnaire. The items were measured by five-point Likert scales in which 1 = "strongly disagree" and 5 = "strongly agree". The demographic data section includes gender, position, years of experience, and country. The questionnaire was reviewed by expert researchers then piloted with a small sample of typical respondents.

The link to the questionnaire was distributed to a convenience sample via two social media platforms (Twitter and WhatsApp), which can be a useful way to reach more participants from different countries and regions. Ultimately, 6 countries participated in the study, as shown in Table III.

TABLE II
SOURCES OF MEASUREMENT ITEMS

Variables	Sources
Perceived Ease of Use	[23] ,[37] ,[35] ,[31] ,[28] ,[17]
Perceived Usefulness	[23] ,[37] ,[35] ,[31] ,[28] ,[17]
User Readiness	[5]
Awareness	[3]
Motivation	[9]
Attitude	[5] ,[17] ,[31] ,[35] ,[28]
Actual use	[28]

TABLE III
DEMOGRAPHIC INFORMATION

Demographic characteristics	Percent
Gender	
Male	83.6
Female	14
Prefer not to say	2.3
Position	
Academic at higher education	43.3
Manager at company or organisation	1.8
Student at higher education	51.5
Student at general education	3.5
Years of experience	
1>	6.4
to 2 1	14
to 3 2	17.5
to 4 3	26.3
to 5 4	9.9
to 6 5	3.5
to 7 6	3.5
to 8 7	5.3
to 9 8	3.5
to 10 9	5.8
10<	4.1

TABLE III
DEMOGRAPHIC INFORMATION *(Continued)*

Demographic characteristics	Percent
Countries	
Saudi Arabia	71.3
United Kingdom	14
Libya	3.5
Canada	4.1
Ireland	3.5
United States	3.5

A total of 171 responses were received. There was a disparity in the response rate between countries, with a response rate of 71.3 per cent from Saudi Arabia, 14 per cent from the United Kingdom, 4.1 per cent from Canada, 3.5 per cent from Libya, 3.5 per cent from Ireland, and 3.5 per cent from the United States. In terms of gender, males formed the largest group of participants at 83.6 per cent, followed by females at 14 per cent; whereas, those who preferred not to say formed 2.3 per cent. With regard to years of experience, respondents varied. The highest rate was 26.3 per cent for those with 3 to 4 years of experience, followed by 17.5 per cent (2 to 3 years), 14 per cent (1 to 2), 9.9 per cent (4 to 5), 6.4 per cent (less than one year), 5.8 per cent (9 to 10), 5.3 per cent (7 to 8), 4.1 per cent (more than 10 years), and 3.5 per cent for those who had 5 to 6 years, 6 to 7 years, and 8 to 9 years of experience. Students in higher education were by far the largest group in terms of position (51.5 per cent), the next largest being academics in higher education positions, at 43.3 per cent. Students in general education and managers in companies or organizations formed comparatively small groups at 3.5 per cent and 1.8 per cent, respectively (see Table III). SPSS (version 27) and SmartPLS software were used to facilitate data analysis for this study.

The authors conducted a pilot study to examine the level of reliability before conducting the main study. They found that the Cronbach's alpha was 0.95, which reflects an excellent level of reliability.

V. Results

This section presents the results of the study, including descriptive statistics, validation tests and structural equation modelling, followed by the discussion section. The subsections below show the results of this analysis.

A. Types of Password Managers that are Used

There are several types of password managers that can be used, the most common of which are shown in Fig. 2.

According to Fig. 2, the commonest type of password manager is the Google Chrome password manager, used by 31% of participants. This is not surprising, and might be due to the widespread use of Google Chrome as a web browser. Keeper Password Manager & Digital Vault is the second most common type, cited by 20% of participants, while LastPass Premium is in third place at 19%. These are followed by Password Boss (12%), RoboForm 8 Everywhere (11%), AgileBits 1 Password (11%), Sticky Password Premium (10%), Danshlane (9%), Zoho Vault (8%), and LogMeOnce Password Management Suite Ultimate (8%).

B. Construct Validity

Construct validity refers to the extent to which a set of items measures the constructs they were designed to measure [19]. This process was established by reviewing previous literature and developing the items. According to Chow et al. [39], items must be significantly loaded to the construct they were designed to measure. Therefore, to make sure these items were properly assigned to their constructs, loading and cross-loading of items were conducted and are presented in Table IV.

C. Convergent Validity

This type of validity requires assessment of three procedures: internal consistency (Cronbach's alpha), composite reliability, and average variance extracted (AVE) [14]. Table V indicates that Cronbach's alpha values ranged from 0.770 to 0.900, which means that items are internally consistent. Composite reliability ranged from 0.866 to 0.937, which is higher than 0.70 as recommended by [25]. Also, average variance extracted (AVE) ranged from 0.619 to 0.881, which is higher than 0.50. Table V also illustrated the results of confirmatory factors analysis (CFA) and ranged from 0.678 to 0.923.

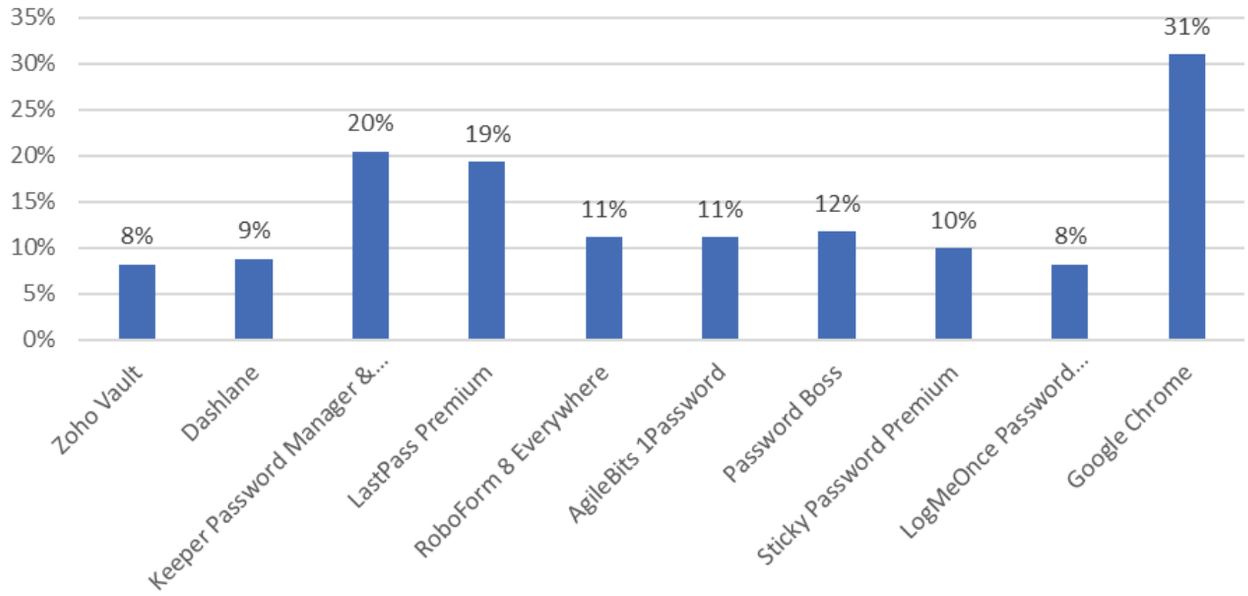

Fig. 2 Types of Password Managers.

TABLE IV
LOADING AND CROSS-LOADINGS OF ITEMS

No.	Variables	Code	AU	AT	AW	MU	PEOU	PU	UR
1	Actual Use	AU_1	0.917	0.741	0.660	0.775	0.702	0.751	0.687
2		AU_2	0.832	0.585	0.451	0.611	0.463	0.572	0.555
3		AU_3	0.733	0.703	0.502	0.592	0.456	0.477	0.578
4	Attitude	AT_1	0.715	0.904	0.726	0.762	0.764	0.662	0.790
5		AT_2	0.702	0.903	0.691	0.685	0.707	0.655	0.735
6		AT_3	0.758	0.837	0.501	0.642	0.525	0.687	0.489
7	Awareness	AW_1	0.588	0.649	0.889	0.676	0.642	0.631	0.516
8		AW_2	0.633	0.768	0.904	0.816	0.809	0.746	0.788
9		AW_3	0.363	0.284	0.678	0.422	0.354	0.347	0.287
10	Motivation to Use	MU_1	0.785	0.774	0.707	0.942	0.618	0.749	0.831
11		MU_2	0.718	0.710	0.800	0.936	0.764	0.756	0.736
12	Perceived Ease of Use	PEOU_1	0.674	0.741	0.709	0.740	0.918	0.682	0.701
13		PEOU_2	0.576	0.674	0.735	0.658	0.930	0.625	0.633
14		PEOU_3	0.429	0.519	0.506	0.460	0.712	0.401	0.274
15	Perceived Usefulness	PU_1	0.671	0.671	0.682	0.735	0.648	0.802	0.566
16		PU_2	0.475	0.624	0.451	0.532	0.443	0.772	0.536
17		PU_3	0.565	0.479	0.573	0.646	0.475	0.711	0.564
18		PU_4	0.568	0.584	0.558	0.585	0.538	0.854	0.625
19	User Readiness	UR_1	0.660	0.691	0.576	0.719	0.586	0.686	0.923
20		UR_2	0.682	0.749	0.648	0.784	0.583	0.658	0.908
21		UR_3	0.672	0.658	0.650	0.783	0.608	0.650	0.907

TABLE V
CONSTRUCTS, ITEMS, AND CONFIRMATORY FACTOR ANALYSIS RESULTS

Variables	Constructs and Items	Factors Loading	Cronbach's Alpha	Composite Reliability	AVE
Actual Use					
	AU_1: I use password managers to keep my passwords.	0.917			
	AU_2: I use password managers to remember my passwords.	0.832	0.770	0.869	0.690
	AU_3: I will make an effort to keep using password managers.	0.733			
Attitude					
	AT_1: Using password managers is a good idea.	0.904			
	AT_2: I like to use password managers to keep my passwords.	0.903	0.857	0.913	0.778
	AT_3: Using password managers is a smart way to remember my passwords.	0.837			

TABLE V
CONSTRUCTS, ITEMS, AND CONFIRMATORY FACTOR ANALYSIS RESULTS *(Continued)*

Variables	Constructs and Items	Factors Loading	Cronbach's Alpha	Composite Reliability	AVE
Awareness					
AW_1: I know how to use password managers.		0.889			
AW_2: I am aware of the benefits of using password managers.		0.904	0.776	0.867	0.688
AW_3: I am aware of the problems that could happen when I use password managers.		0.678			
Motivation to Use					
MU_1: I am motivated to use password managers to keep my passwords.		0.942	0.865	0.937	0.881
MU_2: I see the benefits of using password managers.		0.936			
Perceived Ease of Use					
PEOU_1: The use of password managers is easy for me.		0.918			
PEOU_2: The process of using password managers is clear and understandable.		0.930	0.817	0.893	0.738
PEOU_3: It is easy to create an account in password managers.		0.712			
Perceived Usefulness					
PU_1: Password managers allow me to manage my passwords.		0.802			
PU_2: Password managers help me to remember my passwords.		0.772			
PU_3: Password managers enable me to avoid using one password for all accounts that I have.		0.711	0.793	0.866	0.619
PU_4: It is useful to control all the passwords that I owned.		0.854			
User Readiness					
UR_1: I think that I would be in favor of using password managers.		0.923			
UR_2: I would like to use password managers every time to keep all of my passwords.		0.908	0.900	0.937	0.833
UR_3: I am willing to use password managers.		0.907			

D. Discriminant Validity

Discriminant validity refers to the extent to which constructs differ from each other [31]. According to [31], "discriminant validity was assessed by comparing the square root of the average variance extracted for a given construct with the correlations between that construct and all other constructs." The AVE results were higher than 0.50 and were significant at the 0.001 level. Thus, discriminant validity was supported for all the constructs [15]. (See Table VI).

E. Structural Model

In this stage, the research hypotheses were tested and examined. To conduct this stage, the PLS algorithm and Bootstrapping from SmartPLS software were used. Thus, Fig. 3 represents the measurement model loading, while Fig. 4 shows the structural model.

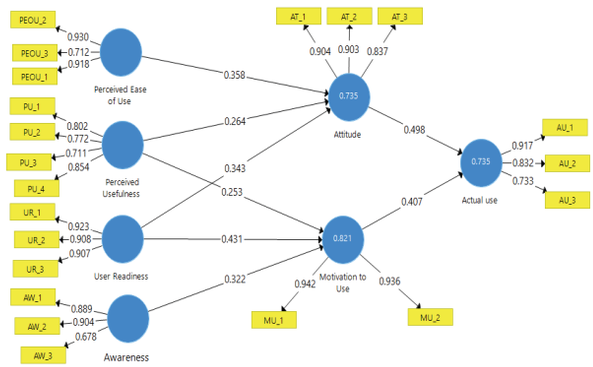

Fig. 3 Path coefficients results.

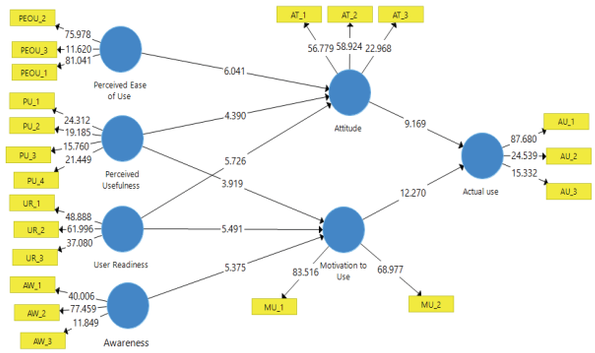

Fig. 4 Path coefficients T values.

Table VII illustrates the results of the research hypotheses test. Regarding the first hypothesis, the relation between perceived ease of use and attitude towards the use of password managers is positive and significant (β = 0.358, t = 6.041, p <0.001). Thus, this result supports this hypothesis. The second hypothesis, concerning the relation between perceived usefulness and attitude towards the use of password managers, is also positive and significant (β = 0.264, t = 4.390, p <0.001). Likewise, the relation between perceived usefulness and motivation to use password managers is positive and significant (β = 0.253, t = 3.919, p <0.001), which supports the third hypothesis. The fourth hypothesis is also supported, as there is a positive and significant relation between user readiness and attitude (β = 0.343, t = 5.726, p <0.001). In the fifth hypothesis, there is a positive and significant relation between user readiness and motivation to use password managers (β = 0.431, t = 5.491, p <0.001). The sixth hypothesis, as analysis shows, is supported, with the relation between awareness and motivation to use password managers being positive and significant (β = 0.322, t = 5.375, p <0.001). Along these lines, the results indicate that there is a possible and significant relationship between attitude and actual use of password managers (β = 0.498, t = 9.169, p <0.001), and this supports the seventh hypothesis. Finally, there is a positive and significant relationship between motivation to use password managers and their actual use (β = 0.407, t = 12.270, p <0.001), which supports the eighth hypothesis.

VI. Discussion

This study investigated the factors that influence the use of password managers. These factors included perceived ease of use, perceived usefulness, user readiness, awareness, attitude, and motivation. The study found that perceived ease of use, perceived usefulness, user readiness, and awareness are important factors related to the use of password managers, and that the actual use of this technology depends on attitude and motivation to use it.

According to [10], perceived ease of use and perceived usefulness are considered the two most important factors that impact the attitude towards acceptance of a new technology. Thus, the high level of belief about the ease of use and usefulness of password managers that has been found in the current study is consistent with previous research which has identified the significant influence of perceived ease of use and usefulness on attitude to-

TABLE VI
Discriminant Validity

Constructs	AU	AT	AW	MU	PEOU	PU	UR
Actual use (AU)	0.831						
Attitude (AT)	0.820	0.882					
Awareness (AW)	0.657	0.730	0.830				
Motivation to Use (MU)	0.801	0.791	0.801	0.939			
Perceived Ease of Use (PEOU)	0.662	0.759	0.766	0.734	0.859		
Perceived Usefulness (PU)	0.731	0.756	0.727	0.801	0.677	0.787	
User Readiness (UR)	0.736	0.768	0.685	0.836	0.649	0.728	0.913

TABLE VII
HYPOTHESES TESTING

H	Relationships	Path	S.E	T.Values	P.Values	Result
H1	Perceived Ease of Use ----------> Attitude	0.358	0.068	6.041	0.000	Supported
H2	Perceived Usefulness ----------> Attitude	0.264	0.068	4.390	0.000	Supported
H3	Perceived Usefulness -------> Motivation to Use	0.253	0.067	3.919	0.000	Supported
H4	User Readiness ------------> Attitude	0.343	0.068	5.726	0.000	Supported
H5	User Readiness ---------> Motivation to Use	0.431	0.067	5.491	0.000	Supported
H6	Awareness --------> Motivation to Use	0.322	0.067	5.375	0.000	Supported
H7	Attitude ---------> Actual use	0.498	0.062	9.169	0.000	Supported
H8	Motivation to Use ---------> Actual use	0.407	0.062	12.270	0.000	Supported

Note: S.E: standard error

wards the use of a new technology [17], [28], [31], [35], [37], [23] and is in line with Davis's argument [10]. Also, the usefulness of password managers for keeping passwords can provide important motivation to use this technology. Thus, perceived usefulness has substantial influence on the motivation to use password managers. This argument aligns with the study conducted by [41].

According to this study's findings, it can be argued that the readiness of users to use password managers is an important factor. The results confirmed that it influenced the users' attitude and motivated them to use it. Therefore, the use of this technology is based on the extent to which the user is ready to use it. This argument is consistent with previous studies. For example, Cheon *et al.* [5] found that readiness is one of the important factors leading to the use of mobile devices for learning.

Another important factor that has been identified by this study is the user's awareness about the use of password managers and the advantages and disadvantages of this use. In other words, it can be argued that if the users are more aware of the use of this technology and its benefits, they will be more motivated to use it. This argument is in alignment with [3], who found that awareness is considered a significant factor influencing the use of Web 2.0 technologies for language learning.

According to the results of this study, it can be confirmed that attitude is also an important factor in the use of password managers. These findings are in agreement with previous studies which established the significant impact of the user's attitude towards the use of new technologies [28], [35], [31], [17], [5]. Despite the importance of this factor in influencing the use of password managers, it is based on the extent to which the use of this technology is easy and useful and the extent to which the user is ready to use it.

The results of this study indicate that motivation is another important factor that influences the use of password managers. The motivation to utilize this technology can be intrinsic (e.g., enjoyment) or extrinsic (e.g., encouragement). This argument is consistent with previous research. For instance, Cullen and Greene [9] argued that extrinsic and intrinsic motivations are influential factors in the use of technology in future teaching.

VII. CONCLUSION

This study investigated the factors that influence the use of password managers. The authors used an online questionnaire for collecting data; for data analysis, they used descriptive statistics to summarize the data; and to test the eight hypotheses conducted in this study they used structural equation modelling. These hypotheses were supported and verified. The results of this study, therefore, indicate that perceived ease of use, perceived usefulness, and user readiness had a positive impact and are substantially associated with attitude which influences the actual use of password managers. Like-

wise, perceived usefulness, user readiness, and awareness had a positive impact and are significantly associated with motivation to use, which also influences the actual use of password managers. Also, the study found that the most commonly used type of password manager was Google Chrome.

In general, it can be argued that the use of password managers is easy and useful. Thus, the users should try it and understand how it can be utilized to get its benefits. So, to obtain any benefits of a new technology such as password managers, the user must be ready, aware, and motivated to go for it and use it. The users also need to improve their attitude towards the technology's use by understanding the benefits and dealing with the problems.

In a practical light, users should understand how to benefit from these tools. They need to practice how to use them more frequently to increase their readiness and awareness towards them. Also, the frequent use of these technologies will make their use easy and useful, which can motivate users to use them effectively.

In summary, it can be concluded that this study makes a useful contribution to the understanding of the factors that influence the use of password managers and how people can be motivated to use them. However, this study, like most research, has limitations, which are listed in the following points.

The use of the questionnaire-based approach provides alternative information, summarizes the data, provides description of the sample, and helps to check the variables and their relationships and the statistical techniques that will be used, but it does not provide a deeper understanding of the context of the use of password managers. Further qualitative research would be useful.

The sample size was an issue in this study. Moreover, the majority of the participants were from one country and one gender. Because of the skewed sample, the results may not be generalizable. However, this was outside the authors' control.

For future work, this study recommends some directions. Researchers may investigate qualitatively how individuals can be encouraged to use this technology. They may also investigate other factors related to security issues in the use of password managers. Another direction can consist of a qualitative focus on why password managers are not used.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone password managers?" in *EuroUSEC 2016 1st Eur. Workshop Usable Secur.*, Darmstadt, Germany, 2016, pp. 1-15, doi: 10.14722/eurousec.2016.23011.

[2] H. Alshahrani and D.R. Pennington, ""How to use it more?" Self-efficacy and its sources in the use of social media for knowledge sharing," *J. Doc.*, vol. 76, no. 1, pp. 231-257, 2019, doi: 10.1108/JD-02-2019-0026.

[3] G. Aşıksoy, "ELT students' attitudes and awareness towards the use of Web 2.0 technologies for language learning," *J. Lang. Linguist. Stud.*, vol. 14, no. 2, pp. 240-251, 2018.

[4] S. Aurigemma, T. Mattson, and L. Leonard, "So much promise, so little use: What is stopping home end-users from using password manager applications?" in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, Hawaii, 2017, pp. 4061-4070. [Online]. Available: http://hdl.handle.net/10125/41650

[5] J. Cheon, S. Lee, S. M. Crooks, and J. Song, "An investigation of mobile learning readiness in higher education based on the theory of planned behavior," *Comput. Educ.*, vol. 59, no. 3, pp.1054-1064, 2012, doi: 10.1016/j.compedu.2012.04.015.

[6] C. Cimpanu, "Crooks Reused Passwords on the Dark Web, so Dutch Police Hijacked Their Accounts," July 27, 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/crooks-reused-passwords-on-the-dark-web-so-dutch-police-hijacked-their-accounts/#:~:text=Police%20gain%20access%20to%20Dream,the%20Hansa%20and%20AlphaBay%20marketplaces. (accessed Mar. 25, 2021).

[7] C. Colby and R. Hodge, "The best password managers of 2021 and how to use them," 2021, [online]. Available: https://www.cnet.com/how-to/best-password-manager (accessed Apr. 3, 2021).

[8] CSID, "CONSUMER SURVEY: PASSWORD HABITS," Sept. 2012. [Online]. Available: https://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf (accessed Apr. 3, 2021).

[9] T. A. Cullen and B. A. Greene, "Preservice Teachers' Beliefs, Attitudes, and Motivation about Technology Integration," *J. Educ. Comput. Res.*, vol. 45, no. 1, pp. 29-47, 2011, doi: 10.2190/EC.45.1.b.

[10] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Q.*, vol. 13, no. 3, pp. 319-340, 1989, doi: 10.2307/249008.

[11] J. R. Evans and A. Mathur, "The value of online surveys," *Internet Res.*, vol. 15, no. 2, pp. 195 – 219, 2005, doi: 10.1108/10662240510590360.

[12] M. Fagan, Y. Albayram, M. Khan, and R. Buck, "An investigation into users' considerations towards using password managers," *Hum. Cent. Comput. Inf. Sci.*, vol. 7, 2017, Art. no. 12, doi: 10.1186/s13673-017-0093-6.

[13] D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," in *Proc. 16th Int. Conf. World Wide Web*, Canada, 2007, MSR-TR-2006-166.

[14] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J. Mark. Res.*, vol. 18, no. 1, pp. 39–50, 1981, doi: 10.2307/3151312.

[15] C. Fornell, G. J. Tellis, and G. M. Zinkhan, "Validity assessment: A structural equations approach using partial least squares," in *Proc. American Mark. Assoc. Educ. Conf.*, 1982.

[16] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proc. 2nd Symp. Usable Priv. Secur.*, USA, 2006, pp. 44-55, doi: 10.1145/1143120.1143127.

[17] I. Gómez-Ramirez, A. Valencia-Arias, and Laura Duque, "Approach to M-learning Acceptance Among University Students: An Integrated Model of TPB and TAM," *Int. Rev. Res. Open Distrib. Learn.*, vol. 20, no. 3, pp. 141-164, Jul. 2019, doi: 10.19173/irrodl.v20i4.4061.

[18] A. Steel, "LastPass Reveals 8 Truths about Passwords in the New Password Exposé," Nov. 2017. [Online]. Available: https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/ (accessed Mar. 25, 2021).

[19] J. F. Hair, W. C. Black, B. J. Babin, R. E. Anderson, and R. L. Tatham, *Multivariate Data Analysis*, 6th Ed., NJ, USA: Prentice-Hall, 1994.

[20] I. Ion, R. Reeder, and S. Consolvo, ""...No one can hack my mind": comparing expert and non-expert security practices," in *SOUPS '15: Proc. 11th USENIX Conf. Usable Priv. Secur.*, Canada, 2015, pp. 327-346.

[21] Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: security analysis of web-based password managers," in *SEC '14: Proc. 23rd USENIX Conf. Secur. Symp.*, CA, USA, 2014, pp. 465-479.

[22] L. M. Ling and C. M. Moi, "PROFESSIONAL STUDENTS' TECHNOLOGY READINESS, PRIOR COMPUTING EXPERIENCE AND ACCEPTANCE OF AN E-LEARNING SYSTEM," *Manag. Account. Rev.*, vol. 6, no. 1, pp. 85-100, 2007, doi: 10.24191/mar.v6i1.505.

[23] S. A. Nikou and A. A. Economides, "Mobile-based assessment: Investigating the factors that influence behavioral intention to use," *Comput. Educ.*, vol. 109, pp. 56-73, 2017, doi: 10.1016/j.compedu.2017.02.005.

[24] M. A. Nugroho, A. Z. Susilo, M. A. Fajar, and D. Rahmawati, "Exploratory Study of SMEs Technology Adoption Readiness Factors," *Procedia Comput. Sci.*, vol. 124, pp. 329-336, 2017, doi: 10.1016/j.procs.2017.12.162.

[25] J. C. Nunnally and I. H. Bernstein, *Psychometric Theory,* NY, USA: McGraw-Hill, 1994.

[26] A. Parasuraman and C. L. Colby, *Techno-Ready Marketing: How and Why Customers Adopt Technology*, NY, USA: Free Press, 2007.

[27] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *SOUPS '19: Proc. 15th USENIX Conf. Usable Priv. Secur.*, USA, 2019, pp. 319-338.

[28] R. A. Sánchez and A. D. Hueros, "Motivational factors that influence the acceptance of Moodle using TAM," *Comput. Hum. Behav.*, vol. 26, no. 6, pp. 1632-1640, 2010.

[29] S. Sarkar, S. Sarkar, K. Sarkar, and S. Ghosh, "Cyber security password policy for industrial control networks," in *2015 1st Int. Conf. Next Gener. Comput. Technol. (NGCT)*, India, 2015, pp. 408-413, doi: 10.1109/NGCT.2015.7375151.

[30] E. Stobert and R. Biddle, "A Password Manager that Doesn't Remember Passwords," in *NSPW '14: Proc. 2014 New Secur. Paradigms Workshop*, USA, pp. 39-52, doi: 10.1145/2683467.2683471.

[31] T. Teo, C. B. Lee, C. S. Chai, and S. L. Wong, "Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: A multigroup invariance analysis of the Technology Acceptance Model (TAM)," *Comput. Educ.*, vol. 53, no. 3, pp. 1000-1009, 2009, doi: 10.1016/j.compedu.2009.05.017.

[32] B. Turner, "Best password managers in 2021: Free and paid software to secure your passwords," 2021. [Online]. Available: https://www.techradar.com/best/password-manager (accessed Apr. 3, 2021).

[33] B. Ur *et al*., ""I added '!' at the end to make it secure": observing password creation in the lab," in *SOUPS '15: Proc. 11th USENIX Conf. Usable Priv. Secur.*, Canada, 2015, pp. 123-140.

[34] R. Wash, E. Rader, R. Berman, and Z. Wellmer, "Understanding password choices: how frequently entered passwords are re-used across websites," in *SOUPS '16: Proc. 12th USENIX Conf. Usable Priv. Secur.*, USA, 2016, pp. 175-188.

[35] F. Weng, R.-J. Yang, H.-J. Ho, and H.-M. Su, "A TAM-Based Study of the Attitude towards Use Intention of Multimedia among School Teachers," *Appl. Syst. Innov.*, vol. 1, no. 3, 2018, Art. no. 36, doi: 10.3390/asi1030036.

[36] J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password memorability and security: empirical results," *IEEE Secur. Priv.*, vol. 2, no. 5, pp. 25-31, Sept.-Oct. 2004, doi: 10.1109/MSP.2004.81.

[37] W. M. Al-Rahmi *et al*., "Big Data Adoption and Knowledge Management Sharing: An Empirical Investigation on Their Adoption and Sustainability as a Purpose of Education," *IEEE Access*, vol. 7, pp. 47245-47258, 2019, doi: 10.1109/ACCESS.2019.2906668.

[38] E. Selevičienė and N. Burkšaitienė, "UNIVERSITY STUDENTS' ATTITUDES TOWARDS THE USAGE OF WEB 2.0 TOOLS FOR LEARNING ESP. A PRELIMINARY INVESTIGATION," *Societal Stud.*, vol. 7, no. 2, pp. 270-291, 2015, doi: 10.13165/SMS-15-7-2-07.

[39] M. Chow, D. K. Herold, T.-M. Choo, and K. Chan, "Extending the technology acceptance model to explore the intention to use Second Life for enhancing healthcare education," *Comput. Educ.*, vol. 59, no. 4, pp. 1136-1144, 2012, doi: 10.1016/j.compedu.2012.05.011.

[40] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*, NJ, USA: Prentice-Hall, 1980.

[41] S.-C. Kong and Y.-Q. Wang, "The influence of parental support and perceived usefulness on students' learning motivation and flow experience in visual programming: Investigation from a parent perspective," *British J. Educ. Technol.*, vol. 52, no. 4, pp. 1749-1770, 2021, doi: 10.1111/bjet.13071.

[42] C. Luevanos, J. Elizarraras, K. Hirschi, and J. Yeh, "Analysis on the Security and Use of Password Managers," in *2017 18th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT)*, Taiwan, 2017, pp. 17-24, doi: 10.1109/PDCAT.2017.00013.

[43] A. Farooq, A Dubinina, S.Virtanen, and J. Isoaho, "Understanding Dynamics of Initial Trust and its Antecedents in Password Managers Adoption Intention among Young Adults," *Procedia Comput. Sci.*, vol. 184, pp. 266-274, 2021, doi: 10.1016/j.procs.2021.03.036.

[44] S. Chaudhary, T. Schafeitel-Tähtinen, M. Helenius, and E. Berki, "Usability, security and trust in password managers: A quest for user-centric properties and features," *Comput. Sci. Rev.*, vol. 33, pp. 69-90, 2019, doi: 10.1016/j.cosrev.2019.03.002.

[45] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv. "Why Older Adults (Don't) Use Password Managers," in *30th USENIX Secur. Symp.*, 2021, pp. 73-90, ISBN. 978-1-939133-24-3.

[46] C. Colby and R. Hodge. "The Best Password Managers for 2022 and How to Use Them," 2022. [online]. Available: https://www.cnet.com/tech/services-andsoftware/best-password-manager (accessed June 8, 2022).