User preference for authentication method: A study on the influencing variables in a web application context

Masjenka L. Veldhuis[a]

[a] *Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands*

ARTICLE INFO

Article history:
Received 00 December 00
Received in revised form 00 January 00
Accepted 00 February 00

Keywords:
Authentication
Identity and Access Management
Preference
Perceptions
MNL model

ABSTRACT

Security provided by authentication methods depends on proper use by people. When people misuse authentication methods, the security of the method degrades, which makes the system more vulnerable to information breaches. People can be stimulated to tolerate security policies of authentication methods when they can use their preferred method. Prior research has examined the overall preference of users for authentication methods, but not the influence of the context, which we focus on in this study. The aim of this study is to evaluate the influence of web applications on preference based on perceptions of web and mobile applications characteristics. The data is collected with a survey and evaluated with a MNL model. The research results reveal that preferences vary between web and mobile applications, and the characteristics can explain these differences in preference. When a web application is perceived to be transferring sensitive information, users prefer to use 2FA. Users who are more familiar with security threats to a web application, are more likely to prefer fingerprint authentication. A next step is to extent the insights in the influence of the context on preference with other types of contexts, for example the identification and authentication at country borders.

1. Introduction

In recent years, organizations have increasingly adopted web applications to offer their services online (ITU, 2017; Talukdar & Gauri, 2011). Web application users are required to register a user account. During the visits of users to their user account, organizations collect and process personal information, which enables them to improve their services and to target customer groups. Due to the disclosure of sensitive personal information, the General Data Protection Regulation (GDPR) enforces organizations to control the access to user accounts (European Commission, 2016). User authentication is in place to control the access.

User authentication is the verification of a user's identity. Once authenticated, the user can gain access to the user account. A variety of authentication methods exists to support the authentication process (O'Gorman, 2003):

- Knowledge-based or something one knows, like the password and Personal Identification Number (PIN).
- Object-based or something one has, like the smartcard.
- Biometric-based or something one is, like fingerprint or facial scan.

Password and PIN are the traditional authentication methods. Currently, the use of biometrics is growing, especially in the banking sector. FinTech experts suggest that biometric and mobile authentication based payment will replace the traditional authentication methods (Fintech Finance, 2017). Different types of authentication methods can also be combined to increase the security strength of the authentication process. This is known as two- or multi-factor authentication (2FA or MFA) (O'Gorman, 2003).

Authentication systems are technologically designed to guarantee security. Next to the technology, security provided by authentication methods depend on how it is utilized by users. Security is degraded when users work around, misuse or avoid the use of authentication, because they perceive the security policy of a method as cumbersome or do to not understand how to use the method (DeWitt & Kuljis, 2006; ISACA, 2018). Human

errors even turn out to account for almost 80% of the security breaches (Braz & Robert, 2006).

Therefore, organizations are looking for strategies to ensure that users follow security policies of authentication methods to prevent security breaches from happening. Users can be stimulated to tolerate these policies when they can use their preferred method. This requires an understanding in the preference for authentication methods of users. Organizations can use this information in their decision-making process for authentication. Designing an authentication system with due care to users can reduce security risks for users, such as privacy invasion or identity theft.

Regarding user accounts, users treat their accounts differently, in a sense that security is given more or less attention. The study of Stobert and Biddle (2018) reveal that the attention to security depends on the type of information disclosed on a user account, especially whether financial information is involved or not (Stobert & Biddle, 2018). While respondents seem to be reluctant with authentication when the disclosed information is not perceived as sensitive (Mahfouz, Muslukhov et al., 2016). Indicating that the preferred authentication method depends on the context.

The contribution of this paper is to examine the influence of the context on preference for authentication methods. Prior studies have investigated preference for authentication methods, but never considered the influence of the context. The aim of this paper is to identify whether preferences of authentication methods differ between web applications, and to identify the variables that explain the difference in preferences.

The structure of this paper is as follows. The next section discusses the related work on authentication and the preference of authentication. In section 3, the conceptual framework for this study is presented, followed by an explanation of the methodology in section 4. Thereafter, the results of the survey and statistical model are discussed. The paper ends with a conclusion and discussion.

2. Related work

2.1. Preferences and perceptions

Preference varies among individuals and situations. The preference model of Timmermans (1982) is applied in this study to explain the unobservable variables that elicit preferences of users, see Figure 1. The decision-making process of a user starts with a decision problem, in this case which authentication method to use, and the user is assumed to be presented a set of alternatives, namely the authentication methods. Each alternative has a number of characteristics, and the objective value of each characteristic gives information on the objective physical environment.

Users are assumed to perform learning and searching processes on authentication. This process depends on user's personal objective characteristics, motivation, and value system, which define together with the decision problem the decision criteria. Users are assumed to be familiar with a few alternative characteristics instead of the finite number of objective characteristics and subjectively evaluate each characteristic. This subjective filter is the perception, which is "individual's beliefs or estimates of the levels of characteristics of the alternatives" (Ben-Akiva et al., 2002). Consequently, the decision-making process of a user is based on the cognitive environment.

The characteristics of each alternative is subjectively evaluated and weighted. The weights indicate the relative importance of the characteristics according to the user. The alternative with the overall highest evaluation represents a user's preference, which is "to choose one alternative above other alternatives" (Ben-Akiva et al., 2002).

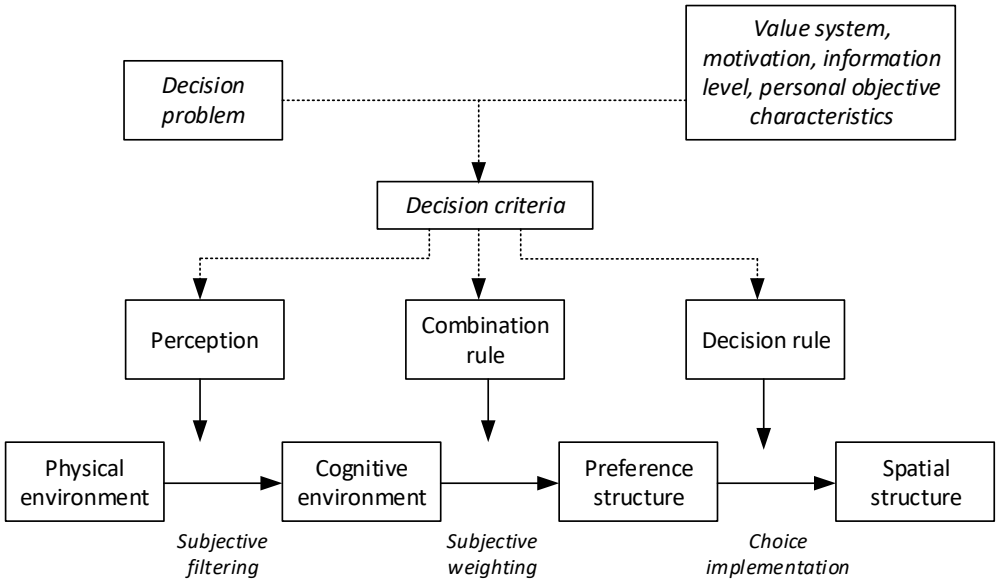

Fig. 1 – Framework for analysis of preferences (Timmermans, 1982).

2.2. Preferences of authentication methods

Prior studies have examined preference for authentication methods. The study of Furnell et al. (2000) is one of the first studies, and combined traditional and biometric authentication methods in the evaluation of preference. Preference is measured by a perceptual rating ranging from "totally acceptable" to "totally unacceptable" and the most preferred method is password despite the shortcomings of the method. Pointed out by the researchers that unfamiliarity of respondents with biometric authentication, might have influenced the results.

The study of Ben-Asher et al. (2011) derive preference from perceptions of security, convenience, and future use of each method. The results reveal that the most preferred method is PIN, while this method is perceived as neither adequate nor convenient. This indicates that inferencing preference from perceptions, does not bring about valid results.

Preference for authentication methods is also examined specifically for e-banking (Weir, Douglas et al., 2009; Weir, Douglas et al., 2010). However, these studies measure preference by perceptions usability, security, and convenience. For that reason, these results can be doubted on their validity.

Another group of studies analyzed preference in the context of smartphones. The research results reveal that users prefer pattern, PIN and password or fingerprint (Mahfouz et al., 2016; Zirjawi, Kurtanovic et al., 2015). The results depend on the type of authentication methods considered, because some studies consider only traditional methods, while other studies look at biometrics. A limited number of studies combine traditional and biometric authentication methods (Al Abdulwahid, Clarke et al., 2015). The latter approach is more relevant for this research, because nowadays users come across traditional and biometric authentication methods.

Preference for authentication methods has been investigated in general, or in context of banking or smartphones. However, the influence of the context on preference has not been considered. The influence might give more information on the variables that users consider in determining their preference for an authentication method. For valid research results, preference is asked directly to users, instead of deriving from perceptions, and traditional together with biometrics are considered. Moreover, the context is represented by web applications. This research makes a start in exploring whether the context contributes in explaining the differences in preferences among users and situations.

3. Conceptual framework

Upon understanding whether preferences vary between different web applications, the hypothesized relations between the independent variables and preference are presented in a conceptual framework, see Figure 2. The independent variables are categorized by:

- Characteristics of the individual.
- Characteristics of the authentication method.
- Characteristics of the web application.

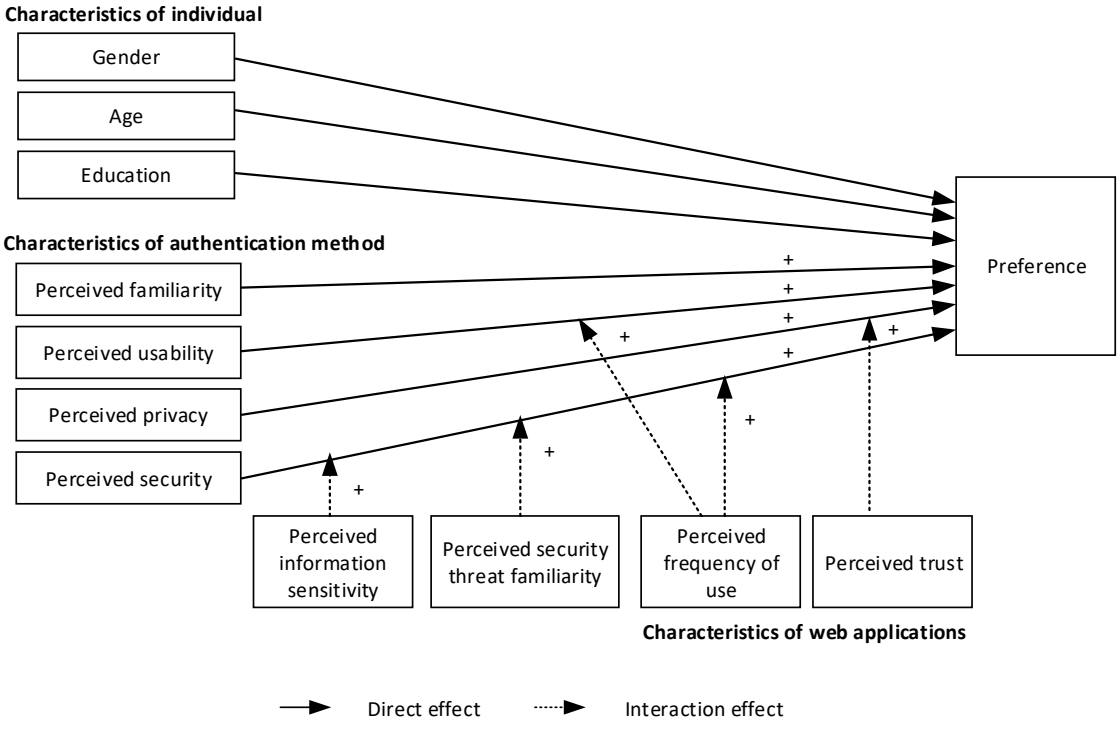

Fig. 2 – Conceptual framework.

3.1. Characteristics of the individual

Socio-demographic characteristics might contribute in explaining the difference in preferences among users. This study is concerned with the characteristics gender, age, and education. Gender is measured by male, female, and neutral resulting in nominal data. Age is measured by year of birth resulting in interval data. Finally, education is measured by the highest level of educational degree according to the Dutch school system, producing ordinal data. No information is available in prior studies, so there is no expectation on the direction of these characteristics. These characteristics are also used to check whether the sample population is representative to the true population.

3.2. Characteristics of authentication methods

The authentication method characteristics consist of familiarity, usability, privacy, and security. In the literature, there is no consensus on the definitions of these concepts. Therefore, the definitions applied in this research is given. Familiarity is defined as "a general feeling of having encountered a person or specific object before, without conscious access to contextual details, such as the time or place of the encounter" (Lee & Kwon, 2011). The study of Clarke et al. (2002) suggest that users prefer a familiar method above unfamiliar methods. For that reason,

perceived familiarity is included to test whether a familiar method is more likely to be preferred by users.

Another characteristic is usability, which is a well-known variable in the literature (Al Abdulwahid et al., 2015; Gunson, Marshall et al., 2011; Zirjawi et al., 2015). Usability is defined as "a set of attributes that bear on the effort needed for use, and on the individual assessment of such use" (Bevan, 1999). Due to the broad definition, the concept is measured by four variables: ease of use, time duration, reliability, and satisfaction. The four variables are combined into one variable "perceived usability" with a factor analysis. Based on prior research, the expectation is that users are more likely to prefer the most usable authentication method.

A third characteristic is privacy, which is concerned with "the individual assessment that the compromise of the database will not enable the adversary to recover the authentication credentials" (Tang, Bringer et al., 2008). Building on previous literature, the expectation is that a method is more likely to be preferred by users when users perceive the method to retain the privacy (Al Abdulwahid et al., 2015; Zirjawi et al., 2015).

The final characteristic is security, which is defined as "the degree to which an individual assesses the ability of an authentication method to prevent unauthorized access, whether accidental or deliberate, to a web application" (Braz, Seffah et al., 2007). The perception of security is suggested by various studies to influence the preference (Weir et al., 2010; Zirjawi et al., 2015). Perceived security is expected to have a positive relation to preference, so a method that is perceived as more secure, is more likely to be preferred by users.

Perceptions are measured by perceptual ratings on perceptual questions (Morikawa, Ben-Akiva, & McFadden, 2002). The perceptual ratings are rated on a 5-point Likert scale. The intervals between the answer options are the same, therefore, the data of the perceptions is interval.

3.3. Characteristics of web applications

This research is concerned with the variables information sensitivity, security threat familiarity, frequency of use and trust as web application characteristic. The study of Forget et al. (2015) suggest that the importance of security depends on the type of user account. Based on these results, the web applications characteristics are considered to influence the contribution of the authentication methods variables on preference. For that reason, the web application characteristics are included as interaction effect in the conceptual model.

Web applications differ in the type of information disclosed on a user account and users can perceive the level of sensitivity of information differently. Prior studies suggest that users are more concerned with security when sensitive information is disclosed to a user account (Ben-Asher et al., 2011; Forget et al., 2015; Stobert & Biddle, 2018). Based on these studies, the expectation is that perceived information sensitivity increases the contribution of perceived security to preference.

Web applications are vulnerable to security threats, whereby the level and type of security threats to web application can differ. The study of Mamonov and Benbunan-Fich (2018) show that exposure to and familiarity with security threats influence the perception of security. Based on this study, the expectation is that perceived security threat familiarity increases the contribution of perceived security to preference.

A third web application characteristic is the frequency of use. For example, Facebook is visited by most users daily. While a user does not make every day a financial transaction online. Frequently accessed user account can collect and process a large amount of personal information, which makes the security strength of the user account more important (Inglesant & Sasse, 2010). In addition, the time required to authenticate can play bigger role when user accounts are frequently accessed (Mamonov & Benbunan-Fich, 2018). Therefore, the expectation is that frequency of use influences the relation between perceived security and preference, and the relation between perceived usability and preference.

During the user interviews, users indicated that trust in the organization behind the web applications plays a role in preferences for authentication methods. Users belief that organizations are responsible to adequately handle and store personal and authentication information. For example, a fingerprint is sensitive information and a compromised fingerprint can be harmful to a user. For that reason, perceived trust is the final web application characteristic and expected to positively relate to perceived privacy and preference.

Like the authentication method variables, the perceptions are measured by perceptual questions rated on a 5-point Likert scale. The variable security threat familiarity is an exception, because this variable is rated on a 3-point Likert scale. The reason is that users are less familiar with security threats, so fewer answer options make

it easier to answer this perceptual question. Furthermore, frequency of use is not rated on a Likert scale, but nine statements are presented to the respondent resulting in ordinal data.

3.4. Preference

Preference is measured by discrete choices involving the alternatives: password, fingerprint, facial scan, password with verification code (2FA), password with fingerprint (2FA), and password with facial scan (2FA). So, preference is categorical. The alternatives are presented among five different web applications. The selected web applications are Facebook, online banking, governmental web application, and health care related web application. The use of mobile banking is rapidly growing, so this mobile application is included as well.

This study aims to answer the following questions:

- Which authentication method do users prefer for different web applications?
- What perceptions of the authentication method characteristics do users have?
- What perceptions of the web application characteristics do users have?
- To what extent do the perceptions of authentication method characteristics and web application characteristics influence the user preference for authentication methods concerning different web applications?

4. Methodology

4.1. Data collection

A survey is used to collect the data on the perceptions and preference. Convenience sampling method is used to recruit the respondents, so the survey is carried out in the Netherlands in 2018 and spread online via WhatsApp, e-mail and Facebook. The population are Dutch citizens, who have at least used one of the selected web applications before. This study is concerned with Dutch users, because one of the selected web applications is only accessible to Dutch citizens. The familiarity with the web applications is to ensure that the data is valid. Without experience, respondents cannot answer the perceptual questions. In addition, the minimum age is 18, because Dutch citizens must arrange services with banks, the government and health care institutions by themselves.

4.2. Survey design

The survey starts with a control question to check whether the respondent has at least visited one of the web applications before. Followed by perceptual questions on the authentication method characteristics and web application characteristics. Thereafter, the respondents are asked to express their preference for one of the six authentication methods. Preference is collected for five web applications. The survey ends with questions on the socio-demographic characteristics of the respondent.

4.3. MNL model estimation

To determine the influence of web applications on preference for authentication methods, a multinomial logit (MNL) model is estimated. MNL is a discrete choice model that allows the dependent variable to be categorical and involving more than two alternatives (McFadden, 1973). The MNL model is derived from the Random Utility theory stating that each alternative provides a perceived utility to a user and preference manifests of the utility-maximizing behavior (Cascetta, 2009). The utility function of an alternative is given by:

$$U_i = V_i + \varepsilon_i = ASC_i + \sum_m \beta_m \cdot x_{mi} + \varepsilon_i \qquad (1)$$

A distinction is made between systematic utility (Vi) and unobserved factors (εi). Systematic utility is assumed to be linear-additive, and this component consists of the elements ASC, β, and x_i. The Alternative Specific Constant (ASC) gives information on the overall differences in utility between alternatives. To evaluate these differences, one alternative is set as reference meaning that the constant of this alternative is fixed to zero. For that reason, a reference alternative has no Alternative Specific Constant (ASC). Another component in the utility function is the taste parameter (β), which indicates the differences in utility between alternative characteristics and is estimated by the maximum likelihood estimation (MLE). Finally, x_{mi} represents the value of the independent variable. Building on the conceptual model, this research considers interaction effects, which can be included in the utility function and estimated by a MNL mode.

The utility of each alternative can be converted into a choice probability for each alternative. The probability function is given by:

$$P(Y = i) = \frac{e^{V_i}}{\sum_J e^{V_j}} \qquad (2)$$

5. Results

5.1. Demographics

A total of 166 completed surveys is obtained. The sample consists of 51,2% female, 48,2% male respondents, and one respondent answered neutral. The age of the respondents ranges between 18-68 years. The largest group is represented by users with an age between 18-25 years, who represent 44% of the respondents. Followed by respondents with the age between 25-35 years, with 23%, and an age between 55-65 years, with 21 %. The smallest group are respondents between 35-45 years, and older than 65, both representing 3% of the respondents. Regarding the education background, this ranges from a low to high educational background. The highly educated people are the largest group, with 70% of the respondents.

5.2. Preferences

Figure 3 shows the results of the preferences, whereby password and password with token authentication are the most preferred authentication methods. Facial scan and password with facial scan are the least preferred authentication methods. Preferences differ between Facebook and the other web applications. For Facebook, the most preferred authentication method is password authentication, while users prefer to use password with token authentication for the other web applications.

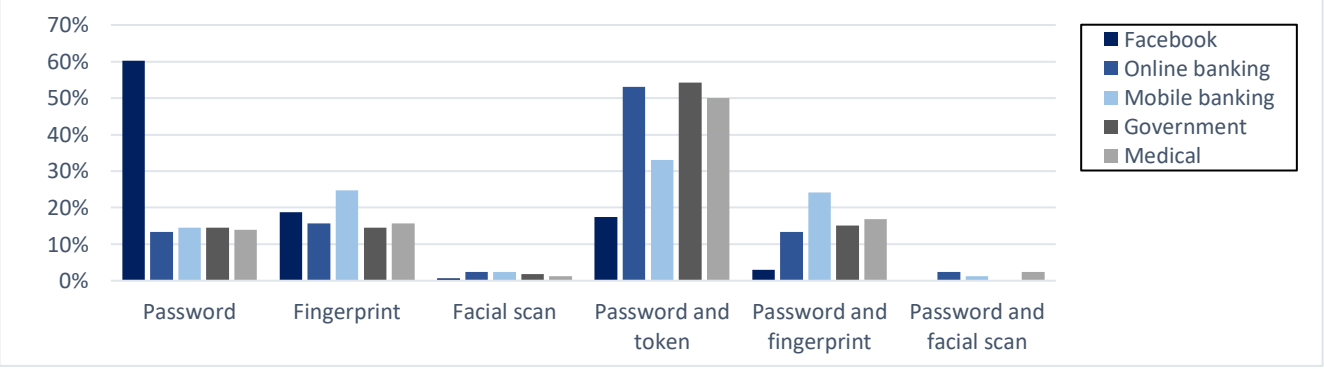

Fig. 3 – Preference for each web application.

5.3. Perceptions

Results on the perceptions of the authentication method characteristics and web application characteristics is displayed in Table 1 and Figure 5. Users are in general familiar with the methods, except for facial scan. Most users have heard of the facial scan, but never used it before. Fingerprint is perceived as most usable due to the ease to use and acceptable time to authenticate. Password is perceived as most reliable. In addition, users seem to have difficulties in expressing their satisfaction with facial scan, because 69% of the respondents answered, "I don't know". The unfamiliarity with facial scan can explain this result. Users have confidence in the privacy of the authentication methods. Finally, the methods are perceived as secure, except for the password. The security of password is perceived as weak.

For the characteristics of the web applications, users perceive most web applications as sensitive, except for Facebook. A reason can be that most users perceive their date of birth and personal interests not as sensitive, which is disclosed on Facebook accounts. While users perceive financial, social security numbers, and medical information as sensitive. Facebook is mostly known for security threats compared to the other web applications. A clarification can be the news exposure of Facebook about the privacy breaches. The frequency of use differs between web applications, whereby Facebook is most frequently visited by users and health care related web applications are least frequently visited. Finally, users perceive the government and health care organization as most trustworthy. Facebook is perceived as untrustworthy. This can also be the result of the news exposure on the privacy breaches.

5.4. MNL model results

The MNL model results are displayed in Table 2 and Figure 4. In general, the authentication methods positively relate to preference, which corresponds to the expectation. This situation does not account for perceived familiarity with 2FA, because the direction of the parameter is negative. Apparently, users are less inclined to prefer 2FA, when they are more familiar with 2FA. A reason could be that users become more aware of the additional effort required to authenticate with 2FA compared to the other methods, which makes 2FA less desirable. Moreover, the contribution of perceived security to the utility of password depends on the perceptions of security threat familiarity.

The direct effects of web application variables reveal that perceived information sensitivity has a positive relation to preference. Indicating that users prefer 2FA when web applications are perceived to be transferring sensitive information. Perceived security threat familiarity also has positive relation to preference. Users who are more familiar with security threats to a web application, are more likely to prefer fingerprint. The frequency of use is transformed into three ordinal levels: low, moderate, and high. A low frequency of use has a positive relation to the utility of fingerprint and 2FA, while a high frequency has a negative relation. Meaning that users prefer 2FA for infrequently visited web applications and change their preference to password authentication when they frequently visit a web application. Perceived trust has a positive relation to preference. However, this parameter is not significant, so this effect is not present in this sample.

The interaction effect of security threat familiarity reveals that the contribution of security is lowered for all three alternatives. A clarification can be that users might have the feeling that they cannot influence the occurrence of a security threat, because even 2FA can be compromised by intruders. For that reason, the perceptions of security are assigned a lower contribution in their preference. Moreover, frequency of use influences the contribution of perceived usability to preference. The contribution of perceived usability to preference is lowered when a web application is infrequently visited but increased for frequently visited web applications. As a result, 2FA is most likely to be preferred by users for infrequently visited web applications, and password authentication for frequently visited web applications.

Finally, the preference differs between users based on the socio-demographic characteristics. Fingerprint is most likely to be preferred by male, older, and lower educated users. While 2FA is more likely to be preferred by younger users. Users with a moderate and high educational background do not have a significantly different preference for authentication methods.

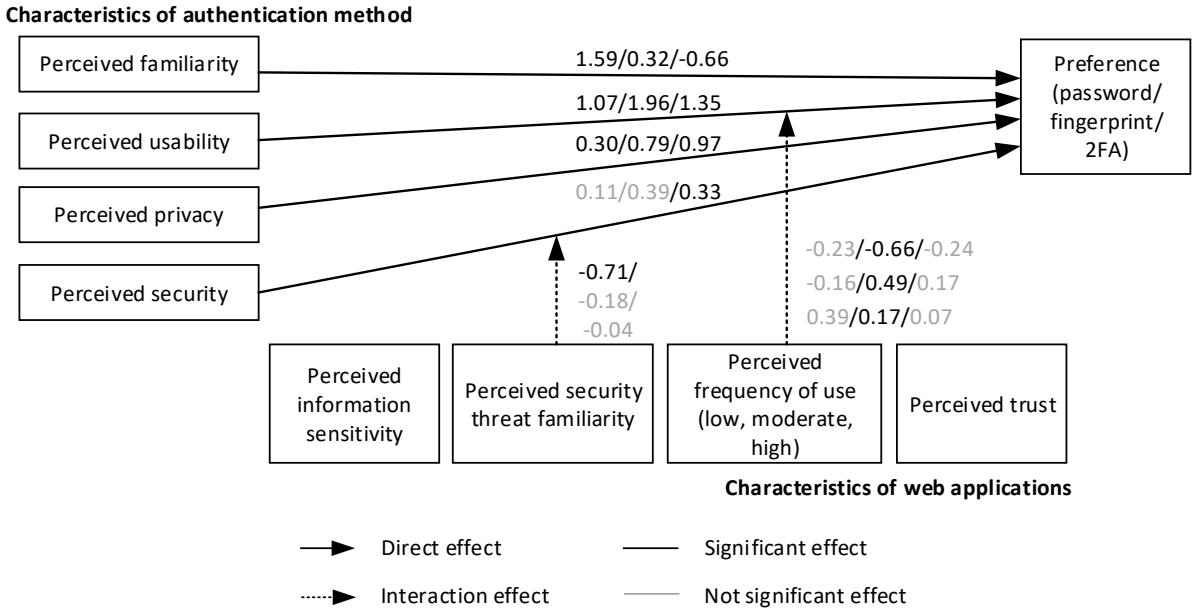

Fig. 4 – Conceptual framework.

6. Conclusion

The aim of this study is to determine whether the context influences preference for authentication methods. According to the results, the overall most preferred authentication method is password with token authentication and the preference of users differ between web applications. For Facebook, users prefer to use password authentication, while password with token authentication is preferred for banking, governmental or health care related web applications.

The results also show that the associations between the perceptions of authentication method characteristics and preference are significant. Users are more likely to prefer a method with which they are familiar or perceive as usable, to preserve their privacy, or be secure. The exception is the familiarity with 2FA, because users are less likely to prefer 2FA, when they are more familiar with this method.

Furthermore, most of the associations between the perceptions of web application characteristics and preference are significant. Perceptions of information sensitivity, security threat familiarity, and frequency of use influence the likelihood that an authentication method is preferred. Users seem to prefer fingerprint when they are familiar with security threats to a web application. In the situation that the information disclosed on a web application is perceived as sensitive or a web application is infrequently visited, users tend to prefer 2FA. Password authentication is preferred for a web application that is frequently visited.

Based on the research results, a recommendation for organizations with a web application is to identify what characterizes their web application and consider these characteristics in the decision-making process for an authentication method. Moreover, the most overall preferred authentication method is 2FA, so a recommendation for the government is to extend the information provision on the use of authentication, especially 2FA, on their digital threat awareness website for society and organizations.

7. Discussion

The study has some limitations that have an impact on the research results. A limitation is the use of convenience sample for the recruitment of respondents. The network of the researcher is bounded to young adults and highly educated users. Consequently, lower educated and older users are underrepresented in the sample meaning that the research results are not generalizable.

Another limitation is the small dataset due to a total of 166 respondents. The preference is collected for five web applications per respondent resulting in a total number of 630 observations to estimate the MNL model. Preferences for facial scan, password with fingerprint, and password with facial scan, are excluded from these observations, because the number of preferences is too limited to estimate the MNL model. Consequently, several parameters are not significant, which might be significant with a larger dataset.

This study considered web applications to represent a context in which authentication occurs. Future research can extend this analysis by considering other types of contexts. This can contribute in getting an understanding of the influence of the context on preference. An interesting context would be the authentication at country borders. This process is regulated nationally and internationally, requires cross-country collaboration, and needs to be accessible for anyone. Moreover, ethical questions might be raised whether individuals are willing to share sensitive personal information with countries that are perceived as untrustworthy or might monitor your behavior without knowing.

Furthermore, this study evaluated preferences for authentication methods based on the random utility theory. There are other choice models that are derived from other theories. Evaluating the preference for authentication methods with another theory and choice model might obtain interesting insights on how users determine their preference. Future research could for example investigate the use of for example the Random Regret model that is built upon the Regret theory.

Appendix A. Perceptions

A.1. Perceptions of interval variables

Table 1 – Perceptions of interval variables.

Variable	Authentication method/ web application	Mean	Standard deviation	Number of "I don't know"
Familiarity	Password	4,42	0,689	0
	Password & token	4,95	0,345	0
	SMS as token	4,30	0,709	0
	Mobile app as token	3,05	1,379	0
	Fingerprint	3,97	1,141	0
	Facial scan	2,54	0,857	0
Easiness	Password	4,06	0,919	0
	Password & token	3,43	1,066	1
	Fingerprint	4,50	0,790	4
	Facial scan	4,01	1,063	19
Reliability	Password	3,93	1,057	1
	Password & token	3,83	1,057	0

	Fingerprint	3,70	1,054	5
	Facial scan	3,15	1,169	26
Time of use	Password	4,01	0,828	0
	Password & token	3,31	0,915	1
	Fingerprint	4,55	0,670	5
	Facial scan	4,12	0,835	26
Satisfaction	Password	3,89	0,917	0
	Password & token	3,73	1,009	4
	Fingerprint	4,04	0,980	33
	Facial scan	3,78	2,291	111
Privacy	Password	4,13	0,833	2
	Password & token	4,06	0,877	2
	Fingerprint	3,84	1,016	11
	Facial scan	3,25	1,116	25
Security	Password	2,48	1,018	2
	Password & token	3,78	0,904	4
	Fingerprint	4,00	0,871	12
	Facial scan	3,78	1,097	23
Threat	Facebook	1,92	0,397	0
familiarity	Online banking	1,66	0,499	0
	Mobile banking	1,51	0,513	0
	Government	1,49	0,513	0
	Medical	1,53	0,513	0
Information	Facebook	3,63	1,114	12
sensitivity	Online banking	4,84	0,593	0
	Mobile banking	4,86	0,585	0
	Government	4,65	0,731	1
	Medical	4,64	0,787	0
Trust	Facebook	2,07	0,919	10
	Banks	3,79	0,887	1
	Government	3,86	0,946	2
	Health care organizations	3,44	0,992	2

A.2. Perceptions of frequency of use

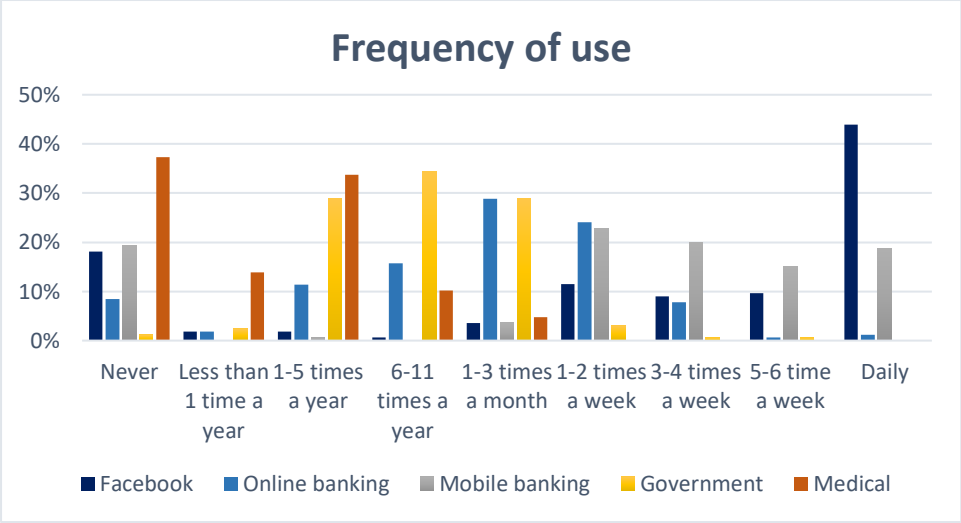

Fig. 5 – Frequency of use for each web application.

Appendix B. MNL estimation

Table 2 – Parameter estimates of MNL model.

Authentication method	Variable	Value	S.E.	T-test	Sig.
Password	ASC	0.00			
	Perceived familiarity	1.59	0.45	3.53	0.00
	Perceived usability	1.07	0.18	6.01	0.00
	Perceived privacy	0.30	0.16	1.91	0.06
	Perceived security	0.11	0.18	0.65	0.52
	Low frequency of use	*0.00*			
	Medium frequency of use	*0.00*			
	High frequency of use	*0.00*			
	Perceived security threat familiarity	*0.00*			
	Perceived information sensitivity	*0.00*			
	Perceived trust	*0.00*			

	Low frequency*perceived usability	-0.23	0.22	-1.05	0.29
	Medium frequency*perceived usability	-0.16	0.22	-0.72	0.47
	High frequency*perceived usability	*0.39*			
	Perceived security threat familiarity*perceived security	-0.71	0.25	-2.84	0.00
	Gender	*0.00*			
	Age	*0.00*			
	Low education	*0.00*			
	Medium education	*0.00*			
	High education	*0.00*			
Fingerprint	ASC	-0.91	1.09	-0.84	0.40
	Perceived familiarity	0.32	0.16	1.97	0.05
	Perceived usability	1.96	0.27	7.29	0.00
	Perceived privacy	0.79	0.20	4.02	0.00
	Perceived security	0.39	0.25	1.58	0.12
	Low frequency of use	0.39	0.27	1.47	0.14
	Medium frequency of use	-0.19	0.27	-0.70	0.48
	High frequency of use	*-0.20*			
	Perceived security threat familiarity	1.12	0.55	2.04	0.04
	Perceived information sensitivity	1.25	0.22	5.83	0.00
	Perceived trust	0.06	0.16	0.34	0.73
	Low frequency*perceived usability	-0.66	0.28	-2.37	0.02
	Medium frequency*perceived usability	0.49	0.30	1.64	0.10
	High frequency*perceived usability	*0.17*			
	Perceived security threat familiarity*perceived security	-0.181	0.37	-0.49	0.62
	Gender	0.48	0.16	2.90	0.00
	Age	0.02	0.01	1.97	0.05

	Low education	1.52	0.63	2.40	0.02
	Medium education	-0.66	0.43	-1.54	0.12
	High education	*-0.86*			
2FA	ASC	2.10	1.01	1.97	0.04
	Perceived familiarity	-0.69	0.19	-3.17	0.00
	Perceived usability	1.35	0.18	7.43	0.00
	Perceived privacy	0.97	0.17	5.74	0.00
	Perceived security	0.33	0.19	1.75	0.08
	Low frequency of use	0.87	0.19	4.64	0.00
	Medium frequency of use	0.40	0.18	2.23	0.03
	High frequency of use	*-1.27*			
	Perceived security threat familiarity	0.27	0.37	0.71	0.48
	Perceived information sensitivity	1.37	0.18	7.84	0.00
	Perceived trust	0.10	0.13	0.76	0.45
	Low frequency*perceived usability	-0.24	0.21	-1.13	0.26
	Medium frequency*perceived usability	0.17	0.22	0.80	0.43
	High frequency*perceived usability	*0.07*			
	Perceived security threat familiarity*perceived security	-0.04	0.28	-0.16	0.87
	Gender	0.15	0.13	1.18	0.24
	Age	-0.02	0.01	-2.24	0.02
	Low education	-0.58	0.46	-1.25	0.21
	Medium education	0.44	0.33	1.36	0.17
	High education	*0.14*			

REFERENCES

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015). Security, privacy and usability – a survey of users' perceptions and attitudes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9264, pp. 153–168). Springer Verlag.

https://doi.org/10.1007/978-3-319-22906-5_12
Ben-Akiva, M., Walker, J., Bernardino, A. T., Gopinath, D. A., Morikawa, T., & Polydoropoulou, A. (2002). *Integration of Choice and Latent Variable Models*. *In Perpetual Motion*. https://doi.org/10.1016/B978-008044044-6/50022-X
Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services - MobileHCI '11*, 465. https://doi.org/10.1145/2037373.2037442
Bevan, N. (1999). Quality in use: Meeting user needs for quality. *The Journal of Systems and Software*, *49*, 89–96.
Braz, C., & Robert, J. (2006). *Security and Usability : The Case of the User Authentication Methods*. *Proceedings of the 18th International Conferenceof the Association - IHM '06*. https://doi.org/10.1145/1132736.1132768
Braz, C., Seffah, A., & M'Raihi, D. (2007). Designing a Trade-Off Between Usability and Security: A Metrics Based-Model (pp. 114–126). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74800-7_9
Cascetta, E. (2009). Transportation Systems Analysis. *Springer Optimization and Its Applications*, *29*, 89–166. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-0-387-75857-2.pdf
Clarke, N. L., Furnell, S. M., Rodwell, P. M., & Reynolds, P. L. (2002). Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, *21*(3), 220–228. Retrieved from https://ac.els-cdn.com/S0167404802003048/1-s2.0-S0167404802003048-main.pdf?_tid=76a67c39-bd45-4fc0-ac62-2ce51d0ad506&acdnat=1528384060_7ee9157319fe09ab2c3d19176644b244
DeWitt, A. J., & Kuljis, J. (2006). Is usable security an oxymoron? *Interactions*, *13*(2), 41–44. Retrieved from http://delivery.acm.org/10.1145/1130000/1125889/p41-dewitt.pdf?ip=145.94.11.157&id=1125889&acc=ACTIVE SERVICE&key=0C390721DC3021FF.512956D6C5F075DE.4D4702B0C3E38B35.4D4702B0C3E38B35&__acm__=1539438586_e7112f5b476ea83c6fef6a21b3b0258a
European Commission. (2016). Directive 95/46/EC (General Data Protection Regulation). Retrieved August 28, 2018, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
Fintech Finance. (2017). Fintech Experts Say Mobile And Biometric Authentication to Replace PINs Within Five Years. Retrieved October 13, 2018, from https://www.fintech.finance/01-news/fintech-experts-say-mobile-and-biometric-authentication-to-replace-pins-within-five-years/
Forget, A., Chiasson, S., & Biddle, R. (2015). Choose Your Own Authentication. In *Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15* (Vol. 8-11-NaN-2015, pp. 1–15). New York, New York, USA: ACM Press. https://doi.org/10.1145/2841113.2841114
Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: a survey of user attitudes. *Computers & Security*, *19*, 529–539. Retrieved from https://ac.els-cdn.com/S0167404800060272/1-s2.0-S0167404800060272-main.pdf?_tid=ce9cc23d-4466-4929-8bd8-7183eb7602fc&acdnat=1539445128_3ead880d1ad9920e153b14b32048e9c4
Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*, 208–220. https://doi.org/10.1016/j.cose.2010.12.001
Inglesant, P. G., & Sasse, M. A. (2010). *The true cost of unusable password policies*. *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. https://doi.org/10.1145/1753326.1753384
ISACA. (2018). Information Security. Retrieved July 20, 2018, from https://www.isaca.org/KNOWLEDGE-CENTER/BMIS/Pages/Business-Model-for-Information-Security.aspx
ITU. (2017). *ICT facts and figures 2017*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
Lee, Y., & Kwon, O. (2011). Intimacy, familiarity and continuance intention: An extended expectation-confirmation model in web-based services. *Electronic Commerce Research and Applications*, *10*(3), 342–357. https://doi.org/10.1016/j.elerap.2010.11.005
Mahfouz, A., Muslukhov, I., & Beznosov, K. (2016). Android users in the wild: Their authentication and usage behavior. *Pervasive and Mobile Computing*, *32*, 50–61. https://doi.org/10.1016/J.PMCJ.2016.06.017
Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44. https://doi.org/10.1016/j.chb.2018.01.028
McFadden, D. (1973). Conditional logit analysis of qualitative choice behavior. *University of California at Berkeley*, 105–142.

Morikawa, T., Ben-Akiva, M., & McFadden, D. (2002). Discrete choice models incorporating revealed preferences and psychometric data. *Advances in Econometrics*, *16*, 29–55. https://doi.org/10.1016/S0731-9053(02)16003-8

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2021–2040. https://doi.org/10.1109/JPROC.2003.819611

Stobert, E., & Biddle, R. (2018). The Password Life Cycle. *ACM Transactions on Privacy and Security*, *21*(3), 1–32. https://doi.org/10.1145/3183341

Talukdar, D., & Gauri, D. K. (2011). Home Internet Access and Usage in the USA: Trends in the Socio-Economic Digital Divide. *Communications of the Association for Information Systems*, *28*(7), 85–98. https://doi.org/10.17705/1CAIS.02807

Tang, Q., Bringer, J., Chabanne, H., & Pointcheval, D. (2008). A formal study of the privacy concerns in biometric-based remote authentication schemes. In *Information Security Practice and Experience* (pp. 56–70). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-79104-1_19

Timmermans, H. (1982). Consumer Choice of Shopping Centre: An Information Integration Approach. *Regional Studies*, *16*(3), 171–182. https://doi.org/10.1080/09595238200185201

Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computer & Security*, *28*, 47–62. Retrieved from https://ac.els-cdn.com/S0167404808000941/1-s2.0-S0167404808000941-main.pdf?_tid=7ce463d0-e04e-42b3-9213-dd3c7c15b33e&acdnat=1528383351_8185a5444ca8fc9698103249bf9d1aa4

Weir, C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers*, *22*(3), 153–164. https://doi.org/10.1016/J.INTCOM.2009.10.001

Zirjawi, N., Kurtanovic, Z., & Maalej, W. (2015). A survey about user requirements for biometric authentication on smartphones. In *2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ESPRE.2015.7330160