Influence of the Perceived Data Security, Operator Credibility and Provider Trust on Usage Frequency of Internet Services

Erik Massarczyk, Peter Winzer
Faculty of Design – Computer Science – Media
RheinMain University of Applied Sciences
Wiesbaden, Germany
Email: erik.massarczyk@hs-rm.de, peter.winzer@hs-rm.de

Abstract—**An increasing customer usage of Internet services with various devices demands a greater effort on data security, credibility and trust issues as due to extensive connections personal data are spread more widely. However, customers often prefer better services rather than higher data security. Here, the aim of this paper is to examine the positive influence of the perceived data security on the usage frequency of Internet services. The main target is to measure how the user (a) perceived data security, (b) perceived operator credibility and (c) perceived trust influence the usage frequency of Internet services. The named variables are analyzed with an adjusted conceptual model based on elements of the Unified Theory of Acceptance and Use of Technology 2. In general, a significant positive influence of a perceived data security on the usage frequency for specific services could be identified. Yet, the perceived trust in the service providers does not significantly relate to a stronger usage frequency of Internet services. Furthermore, for specific Internet services a positive relationship between the user perception about the operator credibility and the usage frequency of the Internet services could be proven. Consequently, customers have data security concerns and these might hinder them to use several Internet services.**

Keywords-data security; trust; credibility; usage frequency; Internet services.

I. INTRODUCTION

The following analysis illustrates the further approach of the already presented study from us regarding the analysis of influence factors of data security and trust on the actual customer usage of Internet services [1].

The growth of the number of Internet services and of the number of users lead to an increased amount of gained data. Especially services like (a) instant messaging, (b) social media, (c) video (broadcasting/streaming), (d) gaming, and (e) cloud computing are used by more and more people with more different devices [2][3][4]. Consequently, the degree of connection of the people and devices increases quite heavily [2]. Based on the growth of the number of connections and Internet services usages, users are generating more personal data that will be distributed to a greater extent [3].

From the customer point of view, it is difficult to comprehend to which extent personal data is collected, where the personal data is stored and which persons get access to the raised personal data for legal or illegal motives [4][5]. Due to the increased connectivity between the devices, unhindered individual communications and marketing measures, a wide range of information and personal data is disclosed. The data disclosure touches the security and privacy concerns of the customers because the personal information could include critical information and intellectual properties of the users. Furthermore, personal information are countable assets from which enterprises as wells as criminals may benefit [2][6][7]. Nonetheless, each user is responsible which data she or he releases for the usage of the specific Internet services and devices. Obviously, many people are willing to distribute their personal information to get a good performance of the used services. Here, they often do not care about risks of data leakages and data misuse.

The rising number of security incidents shows that criminals more frequently attack enterprises, administrations and private customers to get the personal data because they have identified the values of these personal information and intellectual properties [7]. As a result, customers should care more about possible data privacy and security concerns, while using Internet services.

Consequently, we have examined if the private customers perceive any concerns about their own (a) data privacy and (b) data security, and if they have trust and credibility concerns about their application/software providers and their network operators when they use different Internet services with various devices. This study focuses also on the different conditions and usage opportunities between wired and wireless infrastructures and connections, where different types of data security problems could arise. In this respect, we want to measure the status and the perception of data security, while customers using the following services: (a) email, (b) social media, (c) internet telephony, (d) online shopping, (e) cloud computing, (f) e-learning, (g) instant messaging, (h) online banking, (i) navigation, (j) online administration, (j) video on demand, and (k) internet television. Additionally, we analyze the customer evaluation of the credibility in network operators and the trust of the

providers of the named Internet services. Here, it will be measured how the customers perceive that the network operators keep the private data of the customers (credibility) and to what extent the providers of the Internet services (trust) in general further distribute their personal data. Due to customers use the named Internet services differently in the wired and wireless networks, we separate the results in the two named considerations. On the hand, we consider the perceptions in the fixed/wired infrastructure environment and on the other hand, the results in the mobile/wireless infrastructure environment are presented. In the further consideration of the results and discussion, we present the similarities and differences in the usage frequency of the services between the both networks concerning the influence of data security, trust and credibility issues. The also retrieved perceived importance of data security will not be in the major consideration of this study.

In Section II, (a) the term data security, (b) the challenges, (c) the known literature as well as the used conceptual models and research models will be described. Following this section, the methodology, as well as the theoretical approach for carrying out the analysis, will be briefly explained. In Section IV, the results of the hypothesis tests are presented. Finally, in Section V, a critical discussion of the results takes place and a further view on the ongoing research will be done.

II. Literature Review

A. Data Security

In general, the term "data security" describes the secure management of personal data, secure data transmission and the transparency which institutions or persons have access to the personal customer data [6][8]. The correct implementation of data security usually involves that the customers themselves decide who is entitled to access their data. As mentioned in the introduction, customers often ignore possible risks of sharing information and they are not aware of the amount of data, which they produce and which are the consequences if the personal data would be leaked [9]-[11]. The ignorance shows critical issues in three dimensions. Firstly, customers spread personal data which could be linked to confidential information like bank accounts and credit card numbers [9][10]. Secondly, many companies use and transmit – without permission and knowledge of the customers – private customer information, which the customers disclose during the usage of Internet services [12]. Thirdly, as already mentioned, the number of Internet security incidents – like criminal acts of password capturing, eavesdropping and blackmails – have increased quite heavily during the last couple of years [4][7].

B. Challenges

Yet, the perceptions of (a) data security, (b) trust, (c) credibility, (d) sharing of information and (e) risks differs between the individual customers and depend beside others on factors like demography and culture [9]. Therefore, the user attitudes and beliefs are completely subjective and the people have different perceptions about possible risks and prevention of risks [9]. We assume that most of the customers prefer a good Internet service performance instead of strong security or data protection measures. Here, customers frequently do not care about the consequences of misuse and data leakage. Moreover, the providers of Internet services often do not state information about consequences of misuse and data leakage and do not insert different messages to make sure that the users understand the impacts of their data distribution. To increase the customer caution concerning data disclosure, also the providers should implement several measures, which the customers have to comply with to use the services [13].

Especially these issues motivate us to investigate which factors directly influence the usage frequency of Internet services and the individual perception of data security, credibility and trust.

C. Research Model – Adjusted Model with Elements of the Unified Theory of Acceptance and Use of Technology 2

The main target of this study will be to get an increased comprehension of private customer behaviors, especially in the focus on data security, credibility and trust concerns regarding the acceptance and actual usage of services.

The Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) is the direct expansion of the known UTAUT concepts with the factors hedonic motivation, price, and habit/experience, which allows a broader consideration of critical influence factors on user behavior [14]-[17].

Nevertheless, perceived data security, perceived credibility and perceived trust could not be covered by the existing variables of UTAUT2. Nonetheless, an implementation of external variables as influence factors of the user behavior could be performed. By the approach of Escorbar-Rodriguez and Carvajal-Trujillo, the UTAUT2 model is expanded by external variables trust as well as the further components perceived security and perceived privacy [14][18]. This expansion makes clear that the influence of security measures and perceptions on the behavioral intention to use of an innovation can be investigated [14][18]. Furthermore, this approach motivates us to use the factors perceived data security, perceived credibility and perceived trust as external variables in the own adapted model (see Figure 1) [18]. The single analysis of each relation between the named variables with the usage frequency features here the first step of the upcoming regression analyses. As it can be seen in Fig. 1, we also combine the different variables in one regression analysis to figure out how the different variables also affects each other. Each of the analyses will be prepared for each named Internet service, which were already introduced in the first section of this study. The adapted model keeps therefore only the basic idea of the UTAUT2.

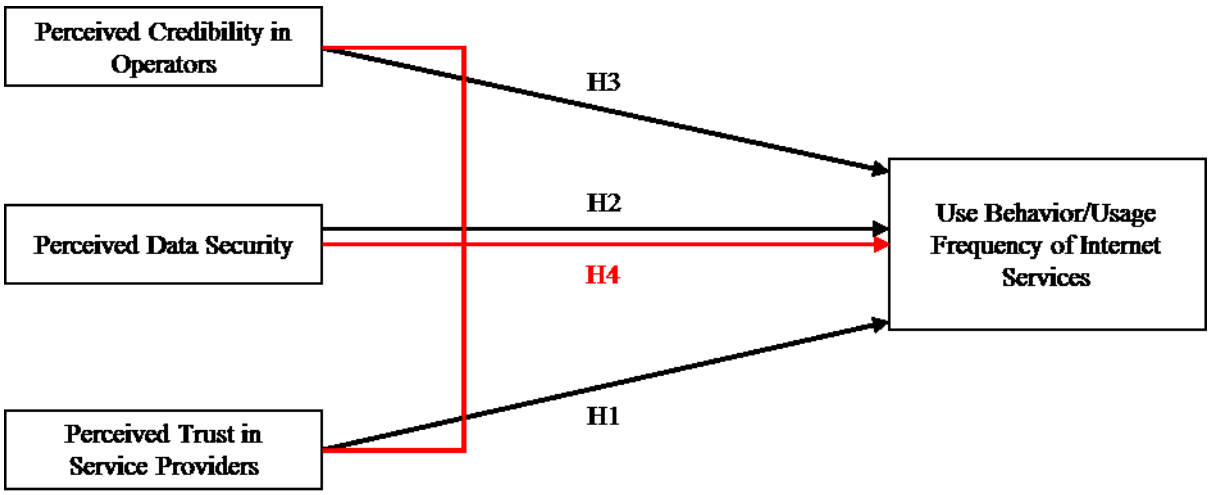

Figure 1. Conceptual Model

As mentioned in the introduction, in comparison to the already presented pre-study, in the further analysis the external variable of perceived credibility of the network operators will be added and further examined [2].

Consequently, we want to measure directly the impact of the perceived data security measures on the actual usage of Internet services (instead of testing the relationship with the behavioral intention to use, as Zhong et al. already did [19]). In other words: The target of investigation is to analyze whether perceived data security, credibility and trust issues lead to a utilization of an Internet service and how the degree of utilization is influenced.

Generally, we estimate that the perception about the increased safety and security of their own data would lead to an increased usage of services. The conceptual model in Fig. 1 bases on the original model of the first presented approach [1]. To support the measurement of the component data security by the customers, the password changing behavior of customers (which is an indicator for the importance of data security) and their relation to the importance of data security will be considered as additional factors. The password changing behavior is therefore relevant to measure if customers with a higher awareness of data security will change their passwords more regularly. We also believe that an outrageous assessment (a) of the proper management of data by network operators and (b) the trustworthiness of service providers would lead to increased use of Internet services.

Perceived credibility describes the users' belief that the used systems would be free of privacy and security threats. In addition, the credibility covers how the customers estimate and perceive the safe storage of their personal information [17].

Customers recognize the behavior of providers if they take care about the personal information and secure transmissions and therefore, if the customers estimate that their personal data are safe [19]-[29]. In case, the operators do not take care about their system, customers perceive the infrastructure as insecure and would avoid to use it.

However, here we definitely want to admit that this point is a pure assumption.

In daily life, people often log into open wireless networks to connect with the Internet and they do not take care or they do not realize the possible threat of data disclosures and linkages. Nevertheless, it could be also the point that the people in the daily life perceive that these infrastructures are secure. Due to these reasons, it is necessary to investigate how the people estimate the security and trustworthiness of their network operators. Furthermore, the customer estimation of the network operators enables a possible assessment of enterprises' trustworthiness and adhere the accepted rules from customer perspective [30]. For this reason, the used survey also includes questions about how the customers perceive the security of the infrastructure and how the network operators use the gained data from the customer. Therefore, we link directly the perceived credibility as positive impact factor for the actual usage of a service, due to the link between the component perceived credibility and a possible behavioral intention to use is already known [18].

Due to the fact that using Internet services (especially mobile services) include security and privacy threats [20], we implement the factor trust. The perception of trust describes how credible the customers perceive the provider [2][18][31][32][33]. The perceived trust of the service providers would be characterized by the fact how the customers estimate the reliability of the service providers in the distribution of personal information to third parties. Based on the assumption that risks and perceived trust directly influence the usage processes [34], the customers would reduce their usage if they expect a loss of privacy and a higher risk in usage [2][35][36][37]. The particular importance of the key factors of risk and trust lies in the fact that these two factors have a major influence on the customer acceptance of innovations (especially mobile payments,

mobile banking and mobile shopping) [19][20][38]-[41]. The trust variable is needed to cover the risk and privacy concerns of the customers and it can be used to figure out how the customers perceive the credible and secure information and experiences of the providers [18][31][32][33]. In addition, trust in a service or in a service provider plays an important role for the customer, since this increases the customer's sense of satisfaction in the service and thus leads to a higher usage frequency [34][42].

Finally, non-existent trust, credibility or the perception of missing security negatively influences customer behavior. An increase in security while using a service would give the customers a more confident secured and satisfied emotion and could possibly imply a stronger usage of this service. Here, previous researches identified that the perceived risk can be seen as one of the key drivers for the estimation of uncertainties in mobile payments, mobile shopping, mobile banking and mobile transactions [35][19][38]-[41], because customers fear possibilities for attacks by mobile transactions and the lack of control. Consequently, customers are paying attention to the products and their providers if they take care about the customers' transactions and personal information security in the usage of mobile payments [19].

Besides mobile banking, mobile payments and mobile shopping, the perceived security issues are even higher in mobile telecommunication networks, due to the fact that mobile networks are shared mediums and different persons can use the same mobile radio cell in the same time. This structure makes the system more vulnerable for attacks within the network [43]. The mobile network operators and providers have to take care about these issues and the introduction of security measures can mitigate uncertainties and risks [44]-[47]. The development of trust in a service is a major aim for customers and providers, because the trust in a service increase the customer convenience and normally leads to a higher performance [34][36][42].

Consequently, the literature conveys the feedback that in several cases trust and the perception of security, risks and uncertainties influence the customer user behavior. All examples and findings demonstrate that possible security issues can significantly negatively influence the intention to use mobile Internet services and therefore, the actual usage frequency could be reduced. Therefore, the authors have set the hypotheses that a better perception in data security leads to an increased usage of services.

Generally, the aim of the analysis is to illustrate how the customers perceive their data security and how they rank the credibility and trust for each Internet service they use. In comparison to the presented relationships between the estimation of perceived security, risks and trust and the usage of mobile banking or mobile payments [21][22], we consider different Internet services for the analysis of the relation between (a) the perceived data security, credibility as well as trust and (b) the usage of services.

Based on these explanations, the hypotheses for this research paper are:

H1: The customer perception of data security has a directly positive effect on the usage of Internet services.

H2: An increased perceived provider trust has a directly positive effect on the usage of Internet services.

H3: An increased perceived network operator credibility has a directly positive effect on the usage of Internet services.

H4: An increased combined perception of trust, credibility and data security has a directly positive effect on the usage of Internet services.

III. METHODOLOGY

The hypotheses are validated based on a current survey. The answers were taken by interviewers in personal interviews, thus ensuring completeness and accuracy of the answers. The respondents were randomly chosen and asked if they wanted to answer the questionnaire. The interviewers were instructed to choose the interviewees as far as possible randomly to make sure to get a sample which represent the demographic characteristics of gender and age of the local population [48][49]. Generally, test persons are asked in December 2016 at public libraries in Wiesbaden (which is a city with approx. 290,000 inhabitants in the middle of Germany) to reach a diversified and representative selection of test persons. In total, the survey includes 290 completed questionnaires. In the first part of the survey, the respondents were asked about their provider and contracts. The second part include questions about the general usage and usage frequency of different Internet services. The subsequent third part of the survey covers the questions on the customer password changing behavior, importance of data security and perceived data security. Questions about perceptions of trust and credibility of providers and operators, as well as on age and gender conclude the survey.

The collected data has been examined based on quantitative research methods with the statistical program SPSS. To evaluate the reliability and validity of the obtained data, Cronbach Alpha was determined and an Exploratory Factor Analysis was performed.

The perceived data security was queried with the question, how the customers perceive their personal data for each specific Internet service in the usage of a fixed and/or mobile Internet access (5-Point-Likert-scale: very secure to very unsecure). For the measurement of the usage frequency of (mobile) Internet services, a 5-Point-Likert-scale (very often to very few) has been used [50]. The perceived credibility (5-Point-Likert-scale: very certain to very uncertain) targets on the question how the customers perceive that the used broadband infrastructure is free of threats. Finally, the trust (5-Point-Likert-scale: very open to very closed infrastructure) is measured by the question whether the users perceive that the Internet service providers spread their personal data without authorization.

As mentioned above, the used approach only keeps elements of the UTAUT2. Therefore, we do not follow the analysis with a Structural Equation Modeling. Instead, we use the ordinary least square regressions to test the significance of each of the named hypotheses [14][15]. In the following combined approach under recognizing and controlling of further variables like importance of data security, perceived credibility and password changing behavior, we use a combined regression analysis.

IV. Data Analysis and Results

A. Result Conditions

The following discussion assumes far predominantly that the participants of the survey answer as private customers, even if it cannot be completely excluded that some of the respondents may also answer from their perspective of personal small enterprises.

We will describe the results of the reliability and validity tests of the overall used hypotheses briefly. After this testing, the regression results of hypotheses will be prioritized to figure out the relationships between (a) perceived data security as well as perceived trust in the service providers and the perceived credibility of network operators and (b) the usage of specific Internet services.

B. Descriptive Results

The results of the second survey presented here extend the original first survey conducted in 2016 and cover 7 additional sets of questions. 55.0% of the respondents are male and the average age of a respondent is between 30 and 39 years. With 48.1%, the group of the 20 and 29-year-olds has the largest share of respondents. Thus, this age group (which is 12.2% of the total population in Germany) is overrepresented in the survey by a factor of four [51]. Based on a study of ARD/ZDF from 2015 the 20 to 29-year-old are nearly 100% Internet users [52].

The over-representation in younger age groups naturally leads to an under-representation of the elder age groups. Consequently, the collected data are not representative. Although there is no representativeness in terms of age and gender, the answers from 290 participants provide much information about the usage behavior of the various communities and thus some conclusions can be drawn on frequency of use and usage preferences. 26.5% of respondents feel confident about their data, but on the contrary, 32.9% of respondents feel more or less insecure about their data. Interestingly, the one third of respondents, who feel insecure in their data security, does not fit at all with the results of the password changing behavior of the customers, since more than 80% of the customers change their passwords much less frequently than once a year: For email accounts 84.3% and for social media accounts 89.2%. Normally, it would be expected that more people change their passwords more regularly if they feel a data insecurity. In this respect, it can be stated as the first conclusion that the perception of the data security does not affect the frequency of the password changes. The reason for this could be that customers are distributing their own data. Therefore, a higher password security increases the overall security, but has no influence the perceived data security. Furthermore, users consider the changing of passwords as cumbersome and not user-friendly.

89.0% of respondents use an anti-virus program, which fit with the quotas of 85.5%, which are also confirmed by studies of the software company McAfee [53]. Most customers associate the use of anti-virus programs with a general increase in data security and often fail to recognize that such programs can only protect the hardware and software from systematic attacks by viruses and malware. However, antivirus programs by their nature do not provide protection against human errors (such as insecure passwords) and thus can only improve data security to a very limited extent.

In average, the customers believe that fixed Internet providers have a little bit safer infrastructure than mobile Internet providers do. Email services are the mostly used services overall (round about 80%). In the fixed infrastructures, about 3/4 of the customers use online shopping, video on demand and online banking (independent from the usage frequency). In the consideration of mobile devices and mobile infrastructures, about 4/5 of the customers use instant messaging.

TABLE I. IMPORTANCE OF DATA SECURITY

Internet Services	Importance of Data Security
Email	54.9% very high importance
Social Media	31.9% very high importance
Online Shopping	53.6% very high importance
Online Banking	75.9% very high importance
Instant Messaging	47.4% very high importance

TABLE II. USAGE FREQUENCY
(Only voting for the highest level of the usage rate)

Internet Services	Usage Frequency
Email	35.1% very frequently
Social Media	43.8% very frequently
Online Shopping	4.9% very frequently
Online Banking	6.9% very frequently
Instant Messaging	63.0% very frequently

TABLE III. TRUST IN SERVICE PROVIDERS

Internet Services	Trust in Data Usage – closed	Trust in Data Usage – open
Email	15.7% very closed	3.9% very open
Social Media	2.1% very closed	21.1% very open
Online Shopping	5.1% very closed	14.1% very open
Online Banking	45.0% very closed	1.7% very open
Instant Messaging	4.6% very closed	14.9% very open

The tables show for the different services: (I) the importance of data security, (II) the usage frequency of Internet services, and (III) confidence in service providers. Interestingly, customers in the services they use very frequently (social media and instant messaging) feel a relatively low data security. Customers also recognize that the providers of these services do not particularly secure the customer data and use it for their own purposes. In opposite, the usage of online banking is relatively rare, but data security is very important to customers in this area, which is, of course, mainly due to the nature of the service and is presumably independent of the channel through which this financial service is provided.

In the consideration of the differences in the perceptions of data security, credibility, trust and usage frequencies of Internet services between women and men, no general diversity can be concluded. However, in the consideration of the difference in means, it can be said that women perceive a lesser degree of data security (women 2.79; men 3.06) and life security (women 3.21; men 3.57) than men do. Despite men feel secure in their life situation, women and men perceive just a neutral data security. This comparison also shows that the general estimation of the data security is less than the general perception about the life security. Therefore, data security worries the respondents and lead to a higher degree of uncertainty.

The view on the data security perceptions of women and men present for the single Internet services presents no difference in means and therefore, we estimate that men and women perceive and treat data security similar. Just in the services online banking and instant messaging, women and men do not perceive similarly in average. Despite men and women estimate secure online banking infrastructures, men estimate a higher data security than women (women 3.57; men 3.98). Contrary, men and women perceive an averagely data security, women have a higher perception of data security for instant messaging services (women 3.13; men 2.67). Interestingly, the credibility of the fixed providers illustrates no difference between women and men. However, the two groups have estimated the credibility of mobile providers quite differently, because women perceive the mobile network operators quite less trustworthy than men.

Table IV illustrates the differences in the usage frequencies between women and men, which presents in general that men use more often Internet services than women do. Due to the significant (below $p<0.05$) F-Ratios about the mark of 1 and 3, the values present a good model fit and describe significant differences in the usage rates of the presented Internet services. The analysis of the means for the other Internet services, which are not included in Table IV, have no significant differences in means.

C. Reliability and Validity

Reliability is a measure of the formal accuracy of surveys/scientific measurements. It is that part of the variance, which can be explained by differences in the characteristic to be measured and not by (measurement) errors. Reliable results must be mainly free of random errors (i.e. reproducibility of results under the same conditions).

The results of the reliability and validity analyses are illustrated in the Tables V and VI. In general, this study includes the following 8 aspects: (1) usage of Internet services (fixed networks), (2) usage of Internet services (mobile networks), (3) usage frequency of Internet services, (4) perceived importance of data security, (5) perceived data security (fixed networks), (6) perceived data security (mobile networks), (7) perceived trust, and (8) perceived credibility.

Generally, all named concepts are examined in the terms of reliability and validity. Following Cronbach, Alpha values must be higher than 0.7 to for a good reliability [54][55][56]. Based on the results in Table V, the collected data for the 7 named aspects are reliable.

TABLE IV. MEAN ANALYSIS FOR USAGE FREQUENCY AND GENDER

Service: Usage Frequency		Mean	F-Ratio	p-significance
Email	female	**3.47**	15.411	**.000**
	male	**4.03**		
Video on Demand	female	**3.35**	4.795	**.029**
	male	**3.69**		
Social Media	female	**3.47**	9.185	**.003**
	male	**4.03**		
Online Banking	female	**2.66**	9.742	**.002**
	male	**3.13**		
Cloud Computing	female	**2.25**	10.611	**.001**
	male	**2.81**		
Instant Messaging	female	**3.95**	6.778	**.010**
	male	**4.38**		
IPTV	female	**3.15**	5.783	**.017**
	male	**3.52**		
Navigation	female	**2.58**	9.064	**.003**
	male	**2.99**		

After the testing of the reliability, the exploratory factor analysis includes the assessment of Kaiser-Meyer-Olkin criterion (KMO), the significance test from Bartlett, and the examination of the cumulative variance to evaluate the validity of the collected data [57]-[61]. Validity considers the consistency of an empirical measurement with the based conceptual/logical measurement concept. To reach a good validity, the concepts should reach significant p values

($p<0.05$) in the Bartlett-Test and KMO values above 0.7 [57]-[61].

Table VI shows good validity scores for the collected data/aspects. The good validity scores are also supported by the results of the cumulative variances higher than 50%, which indicate high explanation rates of the variances of the collected data [58]-[60]. Consequently, the reliability and validity of the collected data are proved. Despite the above-mentioned non-existent representativeness of the collected data, the considered research concepts and scientific questions illustrate that the data could be used for further evaluations.

TABLE V. RELIABILITY ANALYSIS

Research Concepts	Cronbach's Alpha
Usage of Internet Services (fixed networks)	0.780
Usage of Internet Services (mobile networks)	0.784
Usage Frequency of Internet Services	0.803
Perceived Importance of Data Security	0.925
Perceived Data Security (in fixed infrastructures)	0.881
Perceived Data Security (in mobile infrastructures)	0.915
Perceived Trust	0.871
Perceived Credibility	0.772

TABLE VI. VALIDITY ANALYSIS

Research Concepts	KMO	Bartlett-Test	Cumulative Variance
Usage of Internet Services (fixed)	0.825	$p < 0.000$	50.397%
Usage of Internet Services (mobile)	0.804	$p < 0.000$	51.240%
Usage Frequency of Internet Services	0.781	$p < 0.000$	53.724%
Perceived Importance of Data Security	0.901	$p < 0.000$	64.709%
Perceived Data Security (fixed)	0.844	$p < 0.000$	57.791%
Perceived Data Security (mobile)	0.831	$p < 0.000$	62.055%
Perceived Trust	0.827	$p < 0.000$	59.372%
Perceived Credibility	0.709	$p < 0.000$	55.107%

D. Mean Analysis

Next to the reliability and validity analysis and the consideration of the different concepts, as already mentioned in the descriptive results, the survey also covers questions about the usage of anti-virus programs. Due to the nominal coding of the variables of the usage of anti-virus programs, we consider the results based on mean analyses to figure out if the usage of Internet services and the perception of data security differs if the people use anti-virus programs or not. The general view would be that anti-virus programs were normally implemented to create more security for the used systems and that possible threats would be detected and eliminated.

Generally, the (non-)utilization of anti-virus programs does not lead to a significant difference in the perception of data security and the perception of the importance of data security. In addition, if the users utilize an anti-virus program or they refuse to use it, this does not lead to differences in means in the password changing behavior.

The considerations of the decision to use Internet services show normally no differences in mean between people who already use anti-virus programs and people who do not use these services. However, the mean analysis with the help of one factorial analysis of variance (ANOVA) presents a significant difference in means in the usage of email services. Only 63% of the people, who does not use anti-virus programs, utilizes email services. In comparison, 78% of people who have installed anti-virus programs use email services. However, when we add the consideration of the usage frequency under the presented circumstances, there is no significant difference in the usage of email services if the people have an anti-virus program or if they do not have an anti-virus program. Although Internet users want to have a high data security for email services, we cannot finally conclude that the utilization of an anti-virus program will bring a higher security and therefore, the people use more email services. The reason is here that other critical Internet services like online banking or cloud services, which also cover secret details of the private customers, are not influenced by the utilization or non-utilization of anti-virus programs. Therefore, a general impact of anti-virus programs on the perception of data security and the perception of importance of data security cannot be concluded.

The further considerations and analyses of the relations between the named concepts and the conceptual model will be described in the next sub-section.

E. Regression Analyses

As mentioned above, the scope of the study does not allow the testing of all hypotheses.

In the following, at least, the relationship between the factors (a) perceived data security, (b) perceived credibility, (c) perceived trust and the usage frequency of Internet services would be analyzed by means of ordinary least square regressions. The perceived data security is analyzed differently for fixed and mobile Internet services. This differentiation takes account of the fact that the various network/service types have different advantages and disadvantages, and therefore, different utilizations can be expected.

The multiple regression analyses include on the on hand the degree of dependence and on the other hand the grad of the linear relationship (correlation analysis). Independently, if the focus is on the correlation or regression coefficients, in both considerations a 'perfect' relation is expressed by the value 1.000. Nevertheless, correlation/regression coefficients higher than 0.500 symbolize a good interrelation. [60]-[62]

Following the named regression analyses, we combined all possible influence factors of security issues, which have been collected in the survey to analyze their impact on the usage of Internet services.

For this purpose, the perceived data security (= independent variable) is analyzed separately for mobile and fixed broadband infrastructures/services) in relation to the usage frequency of the individual Internet services (= dependent variables); see Table VII.

The r-square values of the individual regressions are quite low, which is mainly due to two causes. On the one hand, only the effects of perceived data security are analyzed for the usage frequency of each service. In each individual case, an r-square for the regression between only an independent variable and a dependent variable is determined. As far as it is assumed, the individual r-squares are not quite as high. On the other hand, the usage frequency of an Internet service does not depend solely on the perceived data security. Based on the estimation of many different influencing factors (some are mentioned in the presented research model), we assume weak regressions, which mean relatively low r-squares.

For the usage of the following services in the fixed and mobile infrastructures, (a) Internet protocol television (IPTV), (b) instant messaging, and (c) online gaming, the customer data security perception does not impact the usage of these services; therefore, the hypothesis H1 cannot be accepted. For the services e-learning and cloud computing, significant positive regression relations could be found for both infrastructures (fixed and mobile). This means that a customer perceives a higher data security in his learning application, he will use the service more frequently. The coefficients of 0.286 (fixed) and 0.370 (mobile) show a quite moderate explanatory rate. As mentioned above, the r-squares of 3.3% (fixed) and 5.7% (mobile) are quite low and describe only a low coefficient of determination. In addition, if customers perceive a higher data security when they use cloud services then they will use them more frequently. Coefficients of 0.330 (fixed) and 0.232 (mobile) and r-squares of 5.8% (fixed) and 2.8% (mobile) shows a moderate explanatory rate and low degree of determination [60]-[62]. For these both services, we do not assume differences in the usage of the services in the both infrastructures and the hypothesis H1 could be accepted.

The analysis of other services (online shopping, online banking, e-mail, social media, and online telephony) shows differences in the results of the regression analyses between mobile or fixed infrastructures. The main reason for differences is the general use of services. Internet users use navigation and social media services twice as frequently by mobile devices in mobile infrastructures in comparison to the fixed-line connections. In contrast, online banking services are used much more frequently via fixed broadband infrastructures.

The perceived data security has only a relatively small (but measurable) influence on the use of navigation services with mobile devices/networks, with regression of 0.161 and r-square of 2.1%. This may be due to the fact that the primary goal of most users of a navigation service is to locate a destination and it is self-evident to them that they may have to make concessions for data security (for example, by authorizing the location).

For fixed networks, positively significant regressions between the perceived data security for (a) emails respectively (b) online banking and the usage of these services could be identified. Despite low r-squares of 5.8% (email) and 5.5% (online banking) and weak regressions, the single coefficients of 0.357 (email) and 0.295 (online banking) represent a moderate regression [60]-[62]. Since emails and, in particular, bank accounts generally contain highly sensitive data from customers, the loss of which can cause considerable damage, customers' need for high data security for these services is particularly high. If the users perceive a better data security for these services, or if the service providers can guarantee their customers a higher data security, they will use these services more frequently.

In addition, email services are often used in professional contact and can contain corresponding confidential information [9][10].

In general, the test of multicollinearities with the Variance Inflation Factor (VIF) shows that all VIF values are below 10 (mostly below 3) and therefore, multicollinearities not exist [57][63][64]. Nonetheless, in some cases, the constants are also significant ($p<0.05$), which could be an indicator for other influence factors or an existing endogeneity. In the further research and examination of the data, we will consider the influence factors and try to figure out which are the indicators for the significant constants.

The relationship of the perceived trust in the service providers (independent variable) and the usage frequency of Internet services (dependent variable) generally show no significant relationship for the specific services. The only exception is online shopping. The positive significant relationship (coefficient = 0.117) shows that customers, who perceive that the shopping providers do not further distribute their personal information, will more frequently use these online shopping platforms.

However, the r-square of 1.7% and the coefficient below 0.200 do not imply a good explanatory rate and the regressive connection seems to be weak [60]-[62]. Generally, the hypothesis H2 about the influence of the customer perception of trust in the service providers of the single specific Internet services on the usage frequency of the specific services cannot be accepted. It seems that trust, as single factor does not have an influence on the customer decision of service usage.

TABLE VII. REGRESSION ANALYSIS – COMPARISON PERCEIVED DATA SECURITY AS INFLUENCE FACTOR FOR USAGE FREQUENCY (single service consideration)

Dependent variables	Independent: Perceived Data Security in Fixed Networks			Independent: Perceived Data Security in Mobile Networks		
	Regression Coefficient B	**Significance**	**R-Square**	**Regression Coefficient B**	**Significance**	**R-Square**
Usage Frequency of Email Services	0.357*	p<0.05	5.8%	No Significance		
Usage Frequency of Cloud Computing Services	0.330*	p<0.05	5.8%	0.232*	p<0.05	2.8%
Usage Frequency of Online Banking Services	0.295*	p<0.05	5.5%	No Significance		
Usage Frequency of E-Learning Services	0.286*	p<0.05	3.3%	0.370*	p<0.05	5.7%
Usage Frequency of Instant Messaging Services	No Significance			No Significance		
Usage Frequency of IPTV Services	No Significance			No Significance		
Usage Frequency of Navigation Services	No Significance			0.161*	p<0.05	2.1%
Usage Frequency of Social Media Services	No Significance			No Significance		
Usage Frequency of Online Gaming Services	No Significance			No Significance		
Usage Frequency of Online Administration Services	0.393*	p<0.05	6.7%	No Significance		
Usage Frequency of Online Shopping Services	No Significance			0.142	p<0.05	1.8%
Usage Frequency of Online Telephony Services	0.228*	p<0.05	2.1%	No Significance		

* The regression presents a significant constant, which could be an indicator for further unconsidered variables or an existing endogeneity, which needs further investigation. Furthermore, the Durban-Watson-Test recognizes a value, which could be an indicator for an existing autocorrelation. To cover the spurious correlations, further investigations must be performed.

A combined regression analysis approach is carried out with the consideration of all of the single data security factors as independent variables in order to analyze the influence the whole impact of perceived data security on the frequency of the user behavior of the specific Internet services. The following variables are controlled: (a) overall perceived data security (in general without any consideration of a single service), (b) perceived importance of data security, (c) perceived credibility of the network operators, and (d) perceived trust in the service providers. The regression analyses for each individual service are carried out separately and shown according to the use of mobile or fixed network services.

The control of the variables that cover security issues (except perceived data security) reveals significant regressive influences of perceived data security on the usage frequency of the specific Internet services (email, cloud computing, online banking and e-learning); see Table VIII.

The control of the variables confirms the results obtained in the first point. When customers use email services over the fixed networks and they feel confident about their data, they will use the data more frequently. Although nearly 80% of the customers use email services over the mobile networks, no significant connection could be found. Despite the non-significance for mobile networks, the regression coefficient of 0.363 for fixed networks shows a moderate explanatory rate [60]-[62]. However, the r-square of 9.7% describes only weak regression with a low coefficient of determination [60]-[62]. The VIF is below 3, so multicollinearities can be excluded [57][63][64]. It seems that customers who experience more data security when using email services will use these services more frequently. This is mainly because customers have stored many confidential information in their email accounts and do not want third parties to have access to these data.

A similar relationship exists for cloud computing: when customers perceive higher data security for cloud computing services, they will use these services more frequently (significantly positive). Despite a moderate regression coefficient of 0.261, the r-square of 8.2% shows a weak regression. The VIF under 3 allows the exclusion of multicollinearities [57][63][64].

The third line of Table VIII represents the influence of the perceived data security on the usage of online banking. It can be identified (for mobile and fixed networks) that users, who have security issues with online banking, do not use online banking. The regression coefficients of 0.218 (fixed) and 0.352 (mobile) describe moderate explanatory rates.

The r-squares of 12.0% (fixed) and 17.7% (mobile) do not imply strong regressions, however, the values are two to three times higher than the r-squares, mentioned above (see Table VIII).

TABLE VIII. REGRESSION ANALYSIS – COMPARISON OF DATA SECURITY AS INFLUENCE FACTOR FOR USAGE FREQUENCY
(combined independent variables consideration on single service consideration)

Dependent variables	Independent: Perceived Data Security in Fixed Networks*			Independent: Perceived Data Security in Mobile Networks*		
	Regression Coefficient B	Significance	R-Square	Regression Coefficient B	Significance	R-Square
Usage Frequency of Email Services	0.363**	p<0.05	9.7%	No Significance		
Usage Frequency of Cloud Computing Services	0.261	p<0.05	8.2%	No Significance		
Usage Frequency of Online Banking Services	0.218	p<0.05	12.0%	0.352	p<0.05	17.7%
Usage Frequency of E-Learning Services	No Significance			0.328	p<0.05	14.5%

* Other independent variables overall perceived data security, perceived importance of data security, perceived credibility of the network operators and perceived trust in the service providers are controlled and implemented.

** The Durban-Watson-Test recognizes a value, which could be an indicator for an existing autocorrelation. To cover the spurious correlations, further investigations must be performed.

These r-squares values describe how much the perceived data security influence the decision how often online banking will be used.

The service e-learning is not used by many customers. Nevertheless, when customers use the service in the mobile environment, the decision to use is influenced by data security issues. The coefficient of 0.328 describes a moderate explanatory rate. The r-square of 14.5% is similar to the results of online banking. Although this regression is classified rather weak, it is still better than most of the regression values found earlier.

For the named services, the hypothesis H1 can be accepted because data security concerns influence the decision to use a service (frequently). However, for the other services (social media, IPTV, online gaming, instant messaging), the hypothesis H1 has to be rejected because an impact of data security issues on the usage of these services could not be (significantly) proved.

Following the considerations of the hypotheses H1 and H2, the hypothesis H3 shall illustrate how the usage frequency of the presented Internet services is affected by the user estimation of the credibility of the network operators for fixed and mobile broadband networks. Table IX visualizes the results for the hypothesis H3, gained from the survey. In this case, only the results, which have shown a significant influence in the model, are presented. For the services email (0.192), navigation (0.184), and online banking (0.210) (see Table IX), only the credibility for the mobile network operators significantly relates to the usage frequency. If the users perceive a higher network credibility, security and trustworthiness, the users will use these services in a higher frequency.

These results match with the results, which were already gained by the analysis for H1. Users have stored personal information in the services email and online banking services and therefore, they are especially looking for a secure access of their own data. For this reason, the users utilize the services in a higher degree when they perceive a higher data security and when the infrastructures are secure, trustworthy and credible.

For the credibility of the fixed network operators, the detected relations cannot be proven. However, all of the three performed regressions, the reached r-squares have values below the 5%. Together with the regression coefficients below 0.3, we have to acknowledge that the explanatory rates of the model are weak. [59]-[61]. However, the decision to use a service is influenced by a couple of different factors. Each of the influence factors show low r-squares when we consider the services solely. The VIF values in the regressions are below 3 and consequently multicollinearities can be excluded [57][63][64]. All regressions have values below 1 in the Durbin-Watson-Test, which means possible autocorrelation issues (like spurious correlations) cannot be excluded for these regressions and further examinations would be necessary.

Despite the critical possible impact factors of autocorrelation and the low values for r-squares and regression coefficients, 75% of the respondents use email and online banking services.

The consideration of the other mentioned Internet services (a) IPTV, (a) online shopping, (c) cloud computing and (d) online gaming shows significant relationships between the credibility of the fixed or mobile network operators and the usage frequency of the named services. Due to the positively significant relations, we expect that the users who perceive a higher trustworthiness and safety in the networks will use these services more frequently than the users without this expectation. The services IPTV (0.276/0.250) and online gaming (0.244/0.256) have coefficients below 0.3 and r-squares below 5% (see Table IX), which means weak regressions and low relationships [59]-[61]. Here, the VIF values are acceptable and multicollinearities can be excluded. However, the two regressions suffer the same problem as the previous considered ones, that the Durbin-Watson-Test show

values around 1. Nonetheless, both services do not face the same problem as the services online banking and email, because both services do not cover the same degree of credible information. Normally, both services give an overview about the actual user behavior, which TV-series or video games the users like and how much time they spend with them. Generally, the usage of these services does not depend on critical information. However, more and more services are combined with stores and online shopping possibilities. Here information about credit cards or personal information may are involved. If we speak about the actual usage of these services, we can fully comprehend that the infrastructures should be secure and transparent, but possible data leakages do not normally lead to the same consequences than if email or online banking accounts have been attacked.

The combination of services with online shopping elements builds the transition to the consideration of the two unconsidered variables, which are also included in Table IX. The services online shopping and cloud computing have r-squares of 7.0% and 8.7% for the analysis of the credibility of the fixed network operators and 5.1% for both analyses for the credibility of mobile network operators. Although the r-squares exceed 5%, we estimate weak regressions. Except the case for the credibility for cloud computing (mobile), the coefficients are below 0.3 and therefore, the credibility influences to a low degree the usage frequency of an Internet service [59]-[61]. Nevertheless, the Durbin-Watson-Test and VIF values are in an acceptable range and so we exclude autocorrelation and multicollinearity issues.

Online shopping and cloud computing also cover critical assets and information like payment information, credit card numbers or enterprise information. Therefore, it can be comprehended that these services have reached slightly better values than the services considered previously. The fact that the credibility of the mobile infrastructure for cloud computing has reached an average rate of explanation shows that the infrastructures used for the two mentioned services should receive the integrity and free attacker entries. Nonetheless, as mentioned above, the results only indicate weak regressive connections and we conclude that other factors are more influencing the usage of the services than the discussed security concerns.

The hypothesis H3 cannot be (fully) rejected or accepted. For the services, which have been presented above, significant weak relationships could be identified and so the hypothesis could be accepted. However, for the other services, which we mentioned in the introduction, relations cannot be concluded and so the hypothesis would be rejected. Consequently, the known linkage between the security patterns of credibility and trust and the behavioral intention, which were already known through the literature [18][21][22], cannot be completely confirmed for the link with actual usage of the service.

To support the previous findings and to expand the results, we will execute another combined regression analysis with the variables, which are used in the first approach above. In the following analysis, we look at perceived credibility with considering the password-changing behavior and perceived importance of data security.

The hypothesis H4 includes the combined analysis of the different security, credibility and trust variables, which have been implemented in the survey. Considering Table X, the dependent variable usage frequency for each specific service depends here directly on the combination of the independent variables.

TABLE IX. COMPARISON PERCEIVED OPERATOR CREDIBILITY INFLUENCE FACTOR FOR USAGE FREQUENCY (single service consideration)

Dependent variables: Usage Frequency	Independent variable: Perceived Credibility of Fixed Network Operators			Independent variable: Perceived Credibility of Mobile Network Operators		
	Regression Coefficient B	Signi-ficance	R-Square	Regression Coefficient B	Signi-ficance	R-Square
Email	No Significance			0.192	p<0.05	2.4%
IPTV	0.276	p<0.05	5.1%	0.250	p<0.05	4.3%
Online Shopping	0.280	p<0.05	7.0%	0.173	p<0.05	2.5%
Cloud Computing	0.281	p<0.05	5.1%	0.361	p<0.05	8.7%
Online Gaming	0.244	p<0.05	3.2%	0.256	p<0.05	3.5%
Navigation	No Significance			0.184	p<0.05	2.8%
Online Banking	No Significance			0.210	p<0.05	3.3%

The implemented independent variables in the model are: (a) perceived data security (single services) in fixed and mobile environments, (b) the general perceived data security, (c) password changing behaviors, (d) perceived importance of data security, (e) perceived credibility of network operators (fixed and mobile), (f) usage of anti-virus programs, and (g) the trust in the providers.

Due to the combined consideration of the variables, higher r-squares can be expected [59]-[61]. Besides the r-squares, the regression coefficients and the F-ratio will be also suitable indicators to present a good feedback about the model fit and the deepness of possible relationships. In the following, we will discuss some of the results, including the examination of H4.

Firstly, email services seem to be directly influenced by the credibility (fixed: -0.289/mobile: 0.289) of the network. However, users who perceive that a mobile infrastructure is free of threats use email services more frequently. Nevertheless, in the consideration in the fixed networks, the user perception is reversed. As shown in Table X, the perception of data security (0.296) also influences the decision how often the service is used. If the users perceive a better data security for emails, they will use the services more often. Despite the r-square of 13% is not quite high and the

coefficients do not exceed 0.3 [59]-[61], the significant F-ratio is above the value of 3.03, which describes a good model fit. The significance of the perceived data security supports the results, which were already got and analyzed in the examination of hypothesis H1. In addition, the significance of the credibility of the mobile network operator positively influencing the usage frequency assists the previously results. The inverse value (-0.289) for the credibility of the fixed network operators makes no sense at first sight. At best, it could be interpreted in such a way that most users now access their emails primarily via mobile networks.

Secondly, the results of cloud computing (0.236) and online banking (0.280) are mostly influenced by the importance of data security. For both services, the data security is important and therefore, when the users perceive this data security they will use this service in a higher frequency. Online banking (0.214) is also influenced by the perceived data security in mobile environments. Therefore, users who perceive a higher data security while using online banking in mobile networks will enhance their usage of this service. Both regressions have r-squares of nearly 20% and symbolize medium explanatory rates. Together with the consideration of the significant F-ratio and F-values above 3, we find a good model fit and that the significant independent variables could well describe the dependent variable usage frequency.

Bearing in mind that the regression coefficients describe a lower degree of relationship. For cloud computing and online banking, we already find several connections between security variables and the usage frequency of these services and all of them are positive. This leads to the conclusion that the users estimate for these services a secure infrastructure, service area and data keeping. If these criteria are fulfilled or at least the customer perceive this status, the users will use the services in a higher frequency.

Considering all results of Table X, we find several influence factors for the usage frequency of Internet services. There is no general influence factor, which influences the usage rate of all services. However, we have to admit that we did not expect this one influence factor at all, because the Internet services are quite different. Nevertheless, a factor, which would be an explanatory factor for the most Internet services, would have been a good result. Concluding, we expect that we cannot generally accept the hypothesis H4, because there is no general influence factor. Otherwise, we see in the model that the variables of the perceived importance of data security (influence factor of 5 services) and operator credibility (influence factor of 4 services) are the major impact variables. For this reason, the hypothesis H4 will not be fully rejected. Several impacts from data security, credibility and trust factors on the development of the usage frequency can be inferred.

Despite the high importance of data security, on the hand, people do not perceive the security of their personal data. This means, the users do not behave in the right way to increase their own personal data security. Although the user estimation of the trust about the service providers how they distribute the data of the users has no influence on the usage frequency of a service, we assume that users have some concerns about service providers about the distribution of personal data. Furthermore, the perception about the credibility and trustworthiness of the networks could possibly influence the customer usage rate of several Internet services. Here, we estimate that most Internet users expect that the Internet infrastructure and the Internet services are free of threats and risks and therefore, these services would be use.

Consequently, our estimation is here that the most Internet users expect that the operators of infrastructure and providers of services take care about the data security of the users. This means the most users do not feel responsible for the security of their own data.

Surely, we do not find general security patterns, which directly relate to the possible user behavior of Internet users. Nonetheless, for specific Internet services several security impact factors and indicators could be found and therefore, it can be assumed that the user behavior and the usage frequency of Internet services are not free of security issues.

V. Conclusions And Future Work

In the journal article, we have analyzed indicators, which influence the decision and usage frequency of Internet services. The focus of the publication is on the effects of perceived data security and perceived trust in the use decision and the usage frequency of Internet services. In the first step, the influence of perceived data security or perceived trust on the usage frequency of certain internet services was examined.

To support the results so far and to expand the results, we have conducted two further analyses. The third one includes the consideration of the impact of perceived credibility on the usage frequency of Internet services. Finally, a combined regression analysis, focusing on the impact of the data security perceived and additional factors by customers on the use of the services were conducted.

It could not be proved in general that security concerns and especially concerns in data security and trust in service providers lead to a reduced or an increased usage of the services. Nonetheless, some evidences and implications for specific services like email, online banking and e-learning exist. Customers, who perceive that their data will be safe, use the service more frequently than customers, who feel uncertain. The main question is why only some of the used services are influenced. We are in the opinion that these developments directly depend on the nature of the service. For example, bank accounts and emails usually contain confidential information, the losses of which can have serious consequences for customers. In contrast, the use of services, such as IPTV merely reveals some information to individual preferences or behaviors. However, most people do not appreciate this information as so critical.

TABLE X. REGRESSION ANALYSIS – COMPARISON OF MODEL FACTORS AS INFLUENCE FACTOR FOR USAGE FREQUENCY
(combined independent variables consideration on single service consideration)

Dependent variable*	Independent variables** Significant parameters	Coefficients	Significance	R-Square	F-Ratio	
					Significance	F-value
Email	Perceived Credibility of Fixed Operator	-0.289	p<0.05	13.0%	p<0.05	3.313
	Perceived Credibility of Mobile Operator	0.289	p<0.05			
	Perceived Data Security (fixed)	0.296	p<0.05			
Cloud Computing	Perceived Importance of Data Security	0.236	p<0.05	20.6%	p<0.05	3.389
Online Banking	Perceived Importance of Data Security	0.28	p<0.05	19.7%	p<0.05	3.458
	Perceived Data Security (mobile)	0.214	p<0.05			
E-Learning	Perceived Importance of Data Security	0.274	p<0.05	18.8%	p<0.05	2.089
Instant Messaging	Perceived Importance of Data Security	0.223	p<0.05	13.2%	p<0.05	2.930
	Password Changing Rate for Emails	-0.227	p<0.05			
IPTV	Password Changing Rate for Emails	-0.241	p<0.05	8.6%	p<0.05	1.472
Navigation	Perceived Credibility of Fixed Operator	-0.197	p<0.05	14.8%	p<0.05	3.068
	Perceived Credibility of Mobile Operator	0.244	p<0.05			
	Perceived Importance of Data Security	0.227	p<0.05			
	Password Changing Rate for Emails	0.219	p<0.05			
Social Media	Usage of Anti-virus programs	0.753	p<0.05	7.7%	p<0.05	1.478
Online Gaming	No Significance					
Online Administration	Perceived Importance of Data Security	0.216	p<0.05	17.8%	p<0.05	1.862
	Perceived Data Security (fixed)	0.333	p<0.05			
Online Shopping	Perceived Credibility of Fixed Operator	0.244	p<0.05	9.5%	p<0.05	1.964
Online Telephony	Perceived Credibility of Mobile Operator	-0.247	p<0.05	13.0%	p<0.05	1.453

* Usage frequency of the single services.
** Perceived data security (single services), password changing behaviors, perceived importance of data security, perceived credibility of network operators, anti-virus usage, perceived data security (general), perceived provider trust.

The second investigation focuses on the perceived trust in service providers. It examines how the transfer of customer data to third parties is evaluated. Interestingly, no evidences for the influence of the perceived trust on the usage of Internet services could be found. It must be predicted that data distributions by the service providers do not affect the user's decision to use a service. This non-existing relation could be explained by the fact that the most people focus on the performance and usability of the Internet services instead of the security, which is mentioned in the second section of this study. Furthermore, it must be assumed that the most people are not aware about these distributions of their data. Therefore, the rejection of this hypothesis is not surprisingly.

The following investigations of the hypotheses H3 and H4 can be well associated with results of the first examination. In general, a full relationship between the factors of the operator credibility in hypothesis H3, the security patterns in the hypothesis H4 and the influence on the usage frequency of Internet services cannot be fully underlined. We show that in some services like online shopping, cloud computing, IPTV and online gaming, that customer perceive the credibility of the networks is free of threats and therefore, it can be directly linked to the usage frequency of the service. In a lower degree, the linkages can also be accepted for the use of email, navigation and online banking services. It can be concluded that the security of the infrastructure is for the use of a couple of services a relevant issue.

In the final hypothesis H4, the usage frequency of an Internet service were directly linked to all of the different security patterns, which were included in the survey. The results present a quite divers field of impact factors for the different Internet services. As mentioned in the section before, there is not one influence factor for all the different Intern services; however, we do did not expect these kind of result. Nonetheless, two security patterns (importance of data security and operator credibility) are influence factors for 50% of the examined Internet services. For this reason, we assume that these two patterns are the major influence factor for user behavior regarding the concerns about data security. As a consequence, these two patterns are more significant than the other factors and so further investigations would be necessary.

Generally, the presented results cannot fully describe the influence of data security, credibility and trust issues on the usage of specific Internet services. However, a general comprehension of the influence of data security behaviors and the trust and credibility of providers and operators would be deepened and for specific Internet services, a relation could be proved. One intension of this study is to present the influence of the providers' reputation on the decision to use an Internet service more frequently, because researchers found out that reputation and credibility of a network and system positively rises the trust in a new application and system like mobile banking [39][44][65][66].

The focus on the assessment of the single influence of data security (and also trust and credibility) on the actual customer usage of Internet services could lead to the problem that the presented approach might not lead to the aimed results, due to the small number of considered concepts.

Consequently, we have presented several differences also in the usage of Internet services and perceptions about data security concerns between the use of the Internet services in mobile and fixed environments. Generally, there does not exist the big difference, however for several services we could find that data security is more important in the mobile than the fixed environment. We estimate here that the most users use these services more and more in the mobile networks and therefore, the perceptions and estimations target more on the mobile environment.

Finally, parts of the differences cannot be explained with the illustrated regression analyses and the considerations of the descriptive statistics, because as already mentioned above, the decision to use an Internet service is quite subjective. Determinants like cultural values, traditions, age, job, obligatory reasons and necessity directly affect usage frequency of an Internet service. Over the time, people normally gain experience with the services. Due to increasing experience, users will develop an increased confidence in the services [17][45][46][47][67]. Consequently, further analyses have to be geared on the analysis of the named factors culture, experience and age and therefore, next surveys and analyses need to test if these factors influence the actual usage of Internet services.

REFERENCES

[1] E. Massarczyk and P. Winzer, "Influence of Perceived Data Security and Trust on the Usage of Internet Services," In S. Böhm, L. Berntzen, and F. Volk (Eds.), The Tenth International Conference on Advances in Human oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 2017, IARIA) [08. - 12. October 2017, Athens]. Conference Proceedings and Thinkmind Library (ISSN: 2308-3492, ISBN: 978-1-61208-592-0)

[2] E. Massarczyk and P. Winzer, "Influence of the Perception of Data Security and Security Importance on Customer Usage of Internet Services," International Journal On Advances in Internet Technology, Thinkmind Library (ISSN: 1942-2652), volume 10, numbers 1 and 2, 2017, pp. 1-22

[3] International Telecommunication Union (ITU), "ICT Facts & Figures – The world in 2015," May 2015, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf, [retrieved: 09.2017]

[4] P. W. Dowd and J. T. McHenry, "Network Security: It's Time to Take It Seriously," Computer (1998), vol. 31, issue 9, IEEE Xplore Digital Library, Sept. 1998, pp. 24-28.

[5] D. Desai, "Law and Technology – Beyond Location: Data Security in the 21st Century," Magazine Communications of the ACM (2013), vol. 56, issue 1, ACM, Jan. 2013, pp. 34-36.

[6] F. S. Ferraz and C. A. Guimarães Ferraz, "Smart City Security Issues: Depicting Information Security Issues in the Role of a urban environment," 7th International Conference on Utility and Cloud Computing, IEEE/ACM, 2014, pp. 842-846.

[7] Kaspersky Lab, "Damage Control: The Cost of Security Breaches," IT Security Risks Special Report Series, https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf., 2015, [retrieved 09.2017]

[8] D. Nayak, N. Rajendran, D. B. Phatak, and V. P. Gulati, "Security Issues in Mobile Data Networks," Vehicular Technology Conference (VTC 2004), vol. 5, IEEE Xplore Digital Library, Sept. 2004, pp. 3229-3233.

[9] S. Dhawan, K. Singh, and S. Goel, "Impact of Privacy Attitude. Concern and Awareness on Use of Online Social Networking," 5th International Conference - Confluence The Next Generation Information Technology Summit 2013, IEEE Xplore Digital Library, Sept. 2014, pp. 14-17.

[10] D. Malandrino, V. Scarano, and R. Spinelli, "How Increased Awareness Can Impact Attitudes and Behaviors Toward Online Privacy Protection," International Conference on Social Computing, IEEE Xplore Digital Library, Sept. 2013, pp. 57-62.

[11] A. N. Joinson. U.-D. Reips, T. Buchanan, and C. B. Paine Schofield, "Privacy, Trust, and Self-Disclosure Online, " Human-Computer Interaction, vol. 25, no. 1, 2010, pp. 1-24.

[12] B. Krishnamurthy, K. Naryshkin, and C. Wills, "Privacy Leakage vs. Protection Measures: the Growing Disconnect," in Web 2.0 Security and Privacy Workshop, 2011, pp. 1-10.

[13] Q. Tan and F. Pivot, "Big Data Privacy: Changing Perception of Privacy, International Conference on Smart City/SocialCom/SustainCom, IEEE, 2015, pp. 860-865.

[14] V. Venkatesh, J. Y. L. Thong, and X. Xin, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," MIS Quarterly, vol. 36, issue 1, 2012, pp. 157-178.

[15] F.-T. Lin, H.-Y. Wu, and T. T. Nguyet Nga, "Adoption of Internet Banking: An Empirical Study in Vietnam," 10th International Conference on e-Business Engnineering, IEEE Xplore Digital Library, 2013, pp. 282-287.

[16] V. Venkatesh, J. Y. L. Thong, and X. Xin, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," MIS Quarterly, vol. 36, issue 1, 2012, pp. 157-178.

[17] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly, vol. 27, issue 3, 2003, pp. 425-478.

[18] T. Escorbar-Rodriguez and E. Carvajal-Trujillo, "Online Purchasing Tickets for Low Cost Carriers: An Application of the Unified Theory of Acceptance and Use of Technology (UTAUT) Model," Tourism Management, vol. 43, 2014, pp. 70-88.

[19] J. Zhong, A. Dhir, M. Nieminen, M. Hämäläinen, and J. Laine, "Exploring Consumer Adoption of Mobile Payments in China," Academic Mind Trek'13, 2013, pp. 318-325.

[20] Y. S. Wang, Y. M. Wang, H. H. Lin, and T. I. Tang, "Determinants of User Acceptance of Internet Banking: an Empirical Study," International Journal of Service Industry Management, vol. 14, 2003, pp. 501-519.

[21] A. Zmijewska, E. Lawrence, R., and R. Steele, "Towards Understanding of Factors Influencing User Acceptance of Mobile Payment Systems," In: Proceedings of the IADIS WWW/Internet, Madrid, Spain, 2004.

[22] T. Dahlberg and A. Öörni, "Understanding Changes in Consumer Payment Habits – Do Mobile Payments and Electronic Invoices Attract Consumers?," In: 40th Annual Hawaii International Conference on System Sciences (HICSS), 2007, p. 50.

[23] P. G. Schierz, O. Schilke, and B. W. Wirtz, "Understanding Consumer Acceptance of Mobile Payment Services: An Empirical Analysis," Electronic Commerce Research and Applications, vol. 9, issue 3, 2010, pp. 209-216.

[24] C. Kim, W. Tao, N. Shin, and K. S. Kim, "An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems," Electronic Commerce Research and Applications, vol. 9, issue 1, 2010, pp. 84-95.

[25] K. Yang, "Exploring Factors Affecting the Adoption of Mobile Commerce in Singapore," Telematics and Informatics, vol. 22 issue 3, 2005, pp. 257-277.

[26] J. Cheong, M. Cheol, and J. Hwang, "Mobile Payment Adoption in Korea," In: ITS 15th biennial conference, Berlin, Germany, 2002.

[27] T. Dahlberg, N. Mallat, and A. Öörni, "Consumer Acceptance of Mobile Payment Solutions," In: G.M. Giaglis (ed.), mBusiness 2003 – The Second International Conference on Mobile Business, Vienna, 2003, pp. 211-218.

[28] N. Mallat, "Exploring Consumer Adoption of Mobile Payments – a Qualitative Study," Mobility Roundtable, Helsinki, Finland, vol. 16, issue 4, 2006, pp. 413-432.

[29] K. Pousttchi and M. Zenker, "Current Mobile Payment Procedures on the German Market from the view of Customer Requirements," In: 14th International Workshop on Database and Expert Systems Applications, 2003, pp. 870-874.

[30] D. Gefen and D. David, "Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers", Database for Advances in Information Systems, vol. 33, issue 3, 2002, pp. 38-53.

[31] R. De Sena Abrahao, S. N. Moriguchi, and D. F. Andrade, "Intention of Adoption of Mobile Payment: An Analysis in the Light of the Unified Theory of Acceptance and Use of Technology (UTAUT)," Innovation and Management Review, vol. 13, 2016, pp. 221-230.

[32] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Initial Trust Formation in New Organizational Relationships," Academy of Management Review, vol. 23, 1998, pp. 473-490.

[33] D. H. McKnight, V. Choudhury, and C. Kacmar, "The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: a Trust Building Model," The Journal of Strategic Information Systems , vol. 11, 2002, pp. 297-323.

[34] T. Zhou, "Understanding Mobile Internet Continuance Usage from the Perspectives of UTAUT and Flow," Information Development vol. 27, 2011, pp. 207-218.

[35] T. Zhou, Y. Lu, and B. Wang, "Integrating TTF and UTAUT to Explain Mobile Banking User Adoption," Computers in Human Behavior, vol. 26, 2010, 760-767.

[36] T. Zhou, "An Empirical Examination of Initial Trust in Mobile Banking," Information Development, vol. 21, issue 5. 2011, pp. 527-540.

[37] A. Y. L. Chong, "Understanding Mobile Commerce Continuance Intentions: An Empirical Analysis of Chinese Consumers," Journal of Computer Information Systems, 2013.

[38] L.-D. Chen, "A Model of Consumer Acceptance of Mobile Payment," International Journal of Mobile Communications, vol. 6, issue 1, 2008, pp. 32-52.

[39] M. A. Mahfuz, L. Khanam, and W. Hu, "The Influence of Culture on M-Banking Technology Adoption: An Integrative Approach of UTAUT2 and ITM," 2016 Proceedings of PICMET'16: Technology Management for Social Innovation, 2016, pp. 70-88.

[40] X. Luo, H. Li, J. Zhang, and J. P. Shim, "Examining Multi-dimensional Trust and Multi-faceted Risk in Initial Acceptance of Emerging Technologies: an Empirical Study of Mobile Banking Services," Decision Support Systems, vol. 49, issue 2, 2010, pp. 222-234.

[41] H.-P. Lu, and P. Y.-J. Su, "Factors Affecting Purchase Intention on Mobile Shopping Websites," Internet Research, vol. 19, issue 4, 2009, pp. 442-458.

[42] T. Oliveira, M. Faria, M. A. Thomas, and A. Popovic, "Extending the Understanding of Mobile Banking Adoption: When UTAUT meets TTF and ITM," International Journal of Information Management, vol. 34, 2014, pp. 689-703.

[43] G. Kim, B. Shin, and H. G. Lee, "Understanding dynamics between Initial Trust and Usage Intentions of Mobile Banking", Information Systems Journal, vol. 19, issue 3, 2009, pp. 283-311.

[44] Y.-H. Chen and S. Barnes, "Initial trust and online buyer behavior", Industrial Management & Data Systems, vol. 107 issue 1, 2007, pp. 21-36.

[45] Y. Lu, S. Yang, P. Y. K. Chau, and Y. Cao, "Dynamics between the Trust Transfer Process and Intention to Use Mobile Payment Services: A Cross-Environment Perspective." Information & Management, vol. 48, issue 8, 2011, pp. 393-403.

[46] Y. Lu, Z. Deng, and B. Wang, "Exploring Factors Affecting Chinese Consumers' Usage of Short Message Service for

Personal Communication", Information Systems Journal, vol. 20, issue 2, 2010, pp. 183-208.

[47] Y. M. Shin, S. C. Lee, B. Shin, and H. G. Lee, "Examining Influencing Factors of Post-Adoption Usage of Mobile Internet: Focus on the User Perception of Supplier-Side Attributes", Information Systems Frontier, vol. 12, issue 5, 2010, pp. 595-606.

[48] J. Bortz and N. Döring, "Research Methods and Evaluations," [German] "Forschungsmethoden und Evaluation; für Human- und Sozialwissenschaftler," Heidelberg, Springer, vol. 4, 2009.

[49] M. Kaya, "Data Collection Procedure", [German] "Verfahren der Datenerhebung," in Albers, S./Klapper, D./Konradt, U./Walter, A./Wolf, J. (Hrsg.): Methodik der empirischen Forschung, Wiesbaden, Gabler, vol. 3, 2013, pp. 49-64.

[50] R. Likert, "A Technique for the Measurement of Attitudes," Archives of Psychology, 1932, pp. 199-224.

[51] Destatis, Statistisches Bundesamt, "Population," [German] "Bevölkerung," [Online] https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Bevoelkerung/Bevoelkerungsstand/Tabellen_/lrbev01.html, 2015, [retrieved 09.2017]

[52] Statista, "Internet Users in Germany from 2001 to 2015," [German] "Anteil der Internetnutzer in Deutschland in den Jahren 2001 bis 2015," [Online]http://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/, 2015, [retrieved: 09.2017]

[53] Statista, "Customers without Anti-Virus Protection," [German], "Anteil der Verbraucher ohne aktives Antivirenprogramm in ausgewählten Ländern weltweit," https://de.statista.com/statistik/daten/studie/226942/umfrage/anteil-der-verbraucher-ohne-aktives-antivirenprogramm/, 2017, [retrieved: 09.2017]

[54] L. J. Cronbach, "Coefficient Alpha and the Internal Structure of Tests," Psychometrika, vol. 16, 1951, pp. 297-334.

[55] C. Fornell and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, vol. 18, issue 1, 1981, pp. 39-50.

[56] R. Hossiep, "Cronbachs Alpha," [German] "Cronbachs Alpha," In Wirtz, M. A. (editor): Dorsch – Lexikon der Psychologie, vol. 17. Verlag Hans Huber, Bern, 2014.

[57] J. F. J. Hair, R. E. Anderson, R. L. Tatham, and W. C. Black, "Multivariate Data Analysis," Macmillan, New York, NY, Macmillan, vol. 3, 1995.

[58] S. Fromm, "Data Analysis with SPSS Part 1," [German] "Datenanalyse mit SPSS für Fortgeschrittene," Arbeitsbuch, vol. 2, VS Verlag für Sozialwissenschaften, GWV Fachverlage, Wiesbaden, 2008.

[59] S. Fromm, "Data Analysis with SPSS Part 2," [German] "Datenanalyse mit SPSS für Fortgeschrittene 2: Multivariate Verfahren für Querschnittsdaten," Lehrbuch, vol. 1, VS Verlag für Sozialwissenschaften, Springer, Wiesbaden, 2010.

[60] N. M. Schöneck and W. Voß, "Research Project," [German] "Das Forschungsprojekt – Planung, Durchführung und Auswertung einer quantitativen Studie," vol. 2. Springer Wiesbaden, 2013

[61] A. Field, "Discovering Statistics Using SPSS," Sage Publications Ltd., vol. 4, 2013.

[62] F. Brosius, "SPSS 8 Professional Statistics in Windows," [German] "SPSS 8 Professionelle Statistik unter Windows," Kapitel 21 Korrelation, International Thomson Publishing, vol. 1, 1998.

[63] D. Lin, D. P. Foster, and L. H. Ungar, "VIF Regression: A Fast Regression Algorithm for Large Data," Journal of the American Statistical Association, vol. 106, issue 493, 2009, pp. 232-247.

[64] S. Petter, D. W. Straub, and A. Rai, "Specifying Formative Constructs in Information Systems Research," MIS Quarterly, vol. 31, issue 4, 2007, pp. 623-656.

[65] C. Flavian, M. Guinaliu, and E. Torres, "The Influence of Corporate Image on Consumer Trust – a Comparative Analysis in Traditional Versus Internet Banking", Internet Research, vol. 15 issue 4, 2005, pp. 447-470.

[66] M. A. Fuller, M. A. Serva, and J. Benamati, "Seeing is Believing: the Transitory Influence of Reputation Information on E-Commerce Trust and Decision Making", Decision Sciences, vol. 38, issue 4, 2007, pp. 675-699.

[67] S. S. Kim and N. K. Malhotra, "A Longitudinal Model of Continued IS Use: An Integrative View of Four Mechanisms Underlying Post-Adoption Phenomena," Management Science vol. 51, issue 5, 2005, pp. 741-755.