Influence of the Perceived Data Security and 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 because the 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 will be to measure how the user perceived data security and perceived trust influences the usage frequency of Internet services. This will be analyzed with an adjusted conceptual model based on elements of the Unified Theory of Acceptance and Use of Technology 2. Generally, a significant positive influence of a perceived data security on the usage frequency for specific services can be found. Yet, the perceived trust in the service providers does not significantly relate to a stronger usage frequency of Internet services. Consequently, customers have data security concerns and these might hinder them to use several Internet services.**

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

I. INTRODUCTION

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 on demand (broadcasting/streaming), (d) gaming, and (e) cloud computing are used by more and more people with more different devices [1][2][3]. Due to this application of services, the degree of connection of the people and devices increases quite heavily [1]. Based on the growth of the number of connections and Internet services usages, the users produce more personal data and the data is spread to a larger degree [2].

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 handle the raised personal data for legal or illegal motives [3][4]. 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 themselves. Furthermore, personal information are countable assets from which enterprises and criminals can benefit [1][5]. Nonetheless, each user is responsible which data he or she releases for the usage of the specific Internet services and the different devices. Obviously, a lot of 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 detected the values of these personal information and intellectual properties [6]. As a result, customers should care more about possible data privacy and security concerns, while using Internet services.

As a consequence, we want to examine if the private customers have data privacy and data security concerns when they use different Internet services with various devices. Together with the different conditions of wired and wireless networks and connections, 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) online 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 add the customer evaluation of the trust of the providers of the named Internet services. Here, it will be measured how the customers perceive that the providers of the Internet services in general further distribute their personal data. Due to customers use the named Internet service 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. Therefore, we implement a variable how the customers perceive the credibility of the network security (operator).

This implementation should just show how the customers estimate the network, but it would not be used for the analysis of the relation to the usage frequency of Internet services.

For this reason, the perception of the credibility of the operator and the importance of data security are falling behind the major considerations of the customer perception

 ISBN: 978-1-61208-592-0

of data security by using Internet services and the trust provider of these services.

In Section II, the term data security, the known literature and used 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 briefly presented. Finally, in Section V, a critical discussion of the results takes place.

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 of which institutions or persons have access to the personal customer data [5][7]. 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 [8][9][10]. 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 [8][9]. Secondly, a lot of companies use and transmit – without permission and knowledge of the customers – private customer information, which the customers disclose during the usage of Internet services [11]. 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 [3][6].

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 [8]. It is also known 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. Especially these behaviors motivate us to investigate which factors directly influence the usage frequency of Internet services and the individual perception of data security and trust.

B. 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 and trust concerns and 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 [12]-[15].

Nevertheless, perceived data security 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 could be expanded by external variables trust as well as the further components perceived security and perceived privacy [12][16]. This expansion makes clear that the influence of security measures and perceptions on the behavioral intention to use of an innovation can be investigated [12][16]. Furthermore, this approach motivates us to use the factors perceived data security and perceived trust as external variables in the own adapted model (see Figure 1) [16]. Therefore, the adapted model keeps only the basic idea of the UTAUT2. In this context, Lin et al. have figured out that data security and privacy are the most affecting factors for an acceptance and adoption of a new technology [13].

Consequently, we want to directly measure 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 [17]). In other words: The target of investigation is to analyze whether perceived data security and trust issues lead to a utilization of an Internet service.

Generally, we estimate that an increased perception for data security measures and trust concerns would lead to an increased usage of services. For the further combined regression analyses, the external variables perceived credibility (operator credibility) and importance of data security are also implemented. Perceived credibility describes the users' belief that the used systems would be free of threats for privacy and security and how the customers estimate and perceive the reliability of the service providers [15]. Customers recognize the behavior of providers if they take care (or if they don´t do so) about the personal information and secure transmissions [17]-[27].

Due to the fact that using Internet services (especially mobile services) include security and privacy threats [18], we implement the factor trust. The perception of trust describes how credible the customers perceive the provider [1][16][28][29][30]. Based on the assumption that risks and perceived trust directly influence the usage processes [31], the customers would reduce their usage if they expect a loss of privacy and a higher risk in usage [1][32][33][34]. 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) [17][18][35]-[38]. 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 [31][39].

 ISBN: 978-1-61208-592-0

Finally, non-existent trust or the perception of missing security negatively impact customer behavior. An increase in security by using a service would give the customers a more confident, secured and satisfied emotion and could possibly imply a stronger usage of this service. 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.

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.

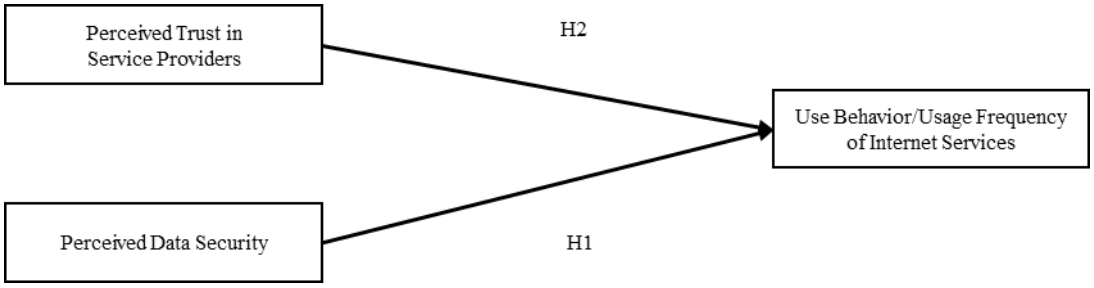

Figure 1. Conceptual Model

III. METHODOLOGY

The hypotheses are validated on the basis of 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 [40][41]. Generally, test persons are asked in December 2016 at public libraries in Wiesbaden (which is a city with approx. 275,000 inhabitants in the middle of Germany) to reach a diversified and representative selection of test persons. In total, the survey includes 290 completed questionnaires. The collected data has been examined based on quantitative research methods with the statistical program Statistical Package for the Social Sciences (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 [42]. Finally, the trust is measured by the question of whether or what users perceive the Internet service providers to spread their personal data (unauthorized).

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 [12][13]. In the afterwards 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 (b) the usage of specific Internet services.

B. Descriptive Results

It could be achieved 290 completed questionnaires. However, the expanded second survey covers 7 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 [43]. Based on a study of ARD/ZDF from 2015 the 20 to 29-year-old nearly 100% Internet users [44].

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.

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 will 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. This could be the reason because a higher password security increases the overall security, but it does not affect the data privacy if the customers distribute their data on their own.

89.0% of respondents use an anti-virus program which fit with the quotas of 85.5%, which are also confirmed by studies by the software company McAfee, which reported 85.5% [45].

In average, the customers believe that fixed Internet providers have a little bit safer infrastructure than mobile Internet providers. 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.

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

The tables show 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.

C. Reliability and Validity

The results of the reliability and validity analyses are illustrated in the Tables IV and V. In general, this study includes the following 7 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), and (7) perceived trust.

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 [46][47][48]. Based on the results in Table IV, the collected data for the 7 named aspects are reliable.

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 [49]-[53]. 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 [49]-[53].

Table V shows good validity scores of the collected data/aspects can be comprehended. The good validity scores are also supported by the results of the cumulative variances higher than 50%, which indicate high explanation rates of the collected data [50][51][52]. Consequently, the reliability and validity of the collected data are proved.

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

 ISBN: 978-1-61208-592-0

TABLE IV. 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

TABLE V. VALIDITY ANALYSIS

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

D. 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 perceived data security, perceived trust and the usage frequency of Internet services will be analyzed by means of ordinary least square regressions. The perceived data security is analyzed differently for the use of 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 also different uses can be expected.

Following the named regression analyses, we combined all possible influence factors of security issues which they have 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 (= independent variables); see Table VI.

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. In so 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), the r-squares cannot be quite so high and we assume weak regressions.

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 if 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. Also, 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 [52][53][54]. 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, 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. Navigation and social media services are used by mobile devices in mobile infrastructures almost twice as frequently as fixed-line connections. In contrast, online banking services are used much more frequently via fixed broadband infrastructures than mobile connections.

The perceived data security has only a relatively small (but measurable) influence on the use of navigation services with mobile devices / networks only weak: 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 emails respectively perceived online banking data security 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 moderate explanatory rates [52][53][54].

Since e-mails 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, of course, particularly high. If the users perceive a better data security for these services, or if the service providers can guarantee their

 ISBN: 978-1-61208-592-0

customers a higher data security, they will use these services more frequently.

TABLE VI. 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.

** 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.

In addition, e-mail services are often used in professional contact and can contain corresponding confidential information [8] [9].

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 [49][55][56]. 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 the service 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 it must be assumed that regressive connection is weak [52][53][54]. 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 must be assumed that trust as single factor does not have an influence on the customer decision of service usage.

Finally, as already mentioned, a combined regression analysis approach is carried out with the implementation of all of the above concepts in order to analyze the influence 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 which cover security issues (except perceived data security) reveals significant regressive

 ISBN: 978-1-61208-592-0

influences of perceived data security on the usage frequency of the specific Internet services (email, cloud computing, online banking and e-learning); see Table VII.

TABLE VII. 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 regression presents a significant constant, which could be an indicator for further unconsidered variables or an existing endogeneity, which needs further investigation.

*** 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.

The control of the variables confirms the results obtained in the first point. When customers use e-mail 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 [52][53][54]. However, the r-square of 9.7% describes only weak regression with a low coefficient of determination [52][53][54]. The VIF is below 3, so multicollinearities can be excluded [49][55][56]. It can be assumed that customers who experience more data security when using e-mail services will use these services more frequently. This is mainly because customers have stored many confidential information in their e-mail 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 [49][55][56].

The third line of Table VII represents the influence of the perceived data security on the usage of online banking. Independently if the customers use online banking in the mobile or fixed networks, it can be identified 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 also 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 VI). These both percentages describe how much the perceived data security declare the decision how often online banking will be used. When people use online banking services, they care about data security issues.

The service e-learning is not used by many customers. But, 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. Despite a normally classified weak regression, this value is better than the results presented above.

To support the previous findings and to expand the results, we have executed a combined regression analysis with the controls of most of the used variables. For the named services, the hypothesis H1 can be accepted because data security concerns impact 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.

V. CONCLUSIONS AND FUTURE WORK

In this paper, 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 a combined regression analysis, focusing on the impact of the data security perceived by customers on the use of the services.

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 e-mails 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.

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 impact 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 data distributions. Therefore, the rejection of this hypothesis is not surprisingly.

To get a better overview, the other relations between the security concerns of data security importance, perceived operator credibility and password changing behavior must be also considered. Consequently, further data analysis and research would be necessary to deepen the current findings.

REFERENCES

[1] 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

[2] 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]

[3] 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.

[4] 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.

[5] 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.

[6] 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]

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[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] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

 ISBN: 978-1-61208-592-0

[22] 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.

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

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

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

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

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

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

[36] 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.

[37] 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.

[38] 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.

[39] 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.

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

[41] 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.

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

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

[44] 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]

[45] 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]

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

[47] 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.

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

[49] 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.

[50] 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.

[51] 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.

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

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

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

[55] 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.

[56] 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.

 ISBN: 978-1-61208-592-0