Examining young users’ security perceptions of mobile banking
A qualitative study on users’ insights about mobile banking.

Authors: Amro Agami
Tiantian Du
Supervisor: Anna-Carin Nordvall
Acknowledgments

We would like to thank and acknowledge several individuals who have assisted and supported us during the process of writing and finalizing this thesis.

We would thank both of our supervisors Dr. Zsuzsanna Vincze for the initial support and input during the first period of the work in addition to Dr Anna-Carin Nordvall also our supervisor who assisted us during the rest of the way with their comments and instruction to make this thesis work.

We also want to thank our participants for their time, effort and input to provide us with the relevant information necessary for our work.

We also want to thank everyone else who supported us during the process of writing the thesis including our family, friends and colleagues around Umeå School of business and economics for exchanging ideas and advices.

Umeå, May 2017

Amro Agami & Tiantian Du
Abstract

The advancement of mobile technology and banking services enabled users to use the mobile banking for variety of tasks with their smartphones, bringing increased flexibility and value-added services to the customers. However, users still have still concerns regarding the security of mobile banking services. The lack of knowledge of the user about different security threats and mechanisms to improve their security represent a major opportunity for hackers and cyberattacks. Despite the fact that the younger students are more knowledgeable about technologies yet awareness is still a concern. Perceived security in the context of young users has not been examined before, although it is considered important in building customer trust. Therefore, this thesis aims to form a good understanding of this topic.

On analysing prior research, the subjects of trust and perceived security in mobile banking is approached by the literature review and an exploratory study that was conducting through qualitative semi-structured interviews. The information collected was carefully analysed with proper tools. After analysing the information an analysis of the literature findings and study finds was presented.

This thesis examined and revealed that perceived security in mobile banking is important for young users. However, it was noticed that users would not leave the service due to their reliance on the bank assurances to cover their security losses, which means that most of the mobile banking young users trust their bank and technology given the security threats. In addition, this study revealed that the majority of users are unaware of security threats surrounding the mobile banking environment. It was found also that the most important mechanism for user is authentication mechanisms.

This thesis provides general understanding of the security in mobile banking. It highlights that perceived security is a complex concept and is affected by various factors such as device, information quality, usage experience and type of network connections. These factors should be carefully considered by users when using the technology. In conclusion, this thesis also implies banks to communicate effectively security information to users in order to avoid mobile banking users’ errors.

Keywords: Perceived security, Mobile banking, User awareness, Authentication
Table of Contents

Chapter 1. Introduction ........................................................................................................ 1
  1.1 Background .................................................................................................................. 1
    1.1.1 Mobile banking technology .................................................................................. 1
  1.1.2 Younger generations: .............................................................................................. 2
  1.1.3 Trust in mobile banking .......................................................................................... 2
  1.1.4 Security in mobile banking ...................................................................................... 3
  1.2 Motivation and knowledge gap .................................................................................... 3
  1.3 Problem discussion ....................................................................................................... 4
  1.4 Research purpose and question ..................................................................................... 5
  1.5 Intended contribution .................................................................................................... 5
  1.7 Thesis disposition ......................................................................................................... 5

Chapter 2: Theoretical background ...................................................................................... 7
  2.1 Related definitions ......................................................................................................... 7
    2.1.1 Security and mobile banking .................................................................................. 7
    2.1.2 Threats to mobile banking security ........................................................................ 8
  2.2 Trust concepts ............................................................................................................... 9
    2.2.1 Trust in technology ............................................................................................... 10
    2.2.2 Institution based trust ........................................................................................... 11
    2.2.3 Trusting beliefs .................................................................................................... 12
    2.2.4 Trusting intentions ............................................................................................... 13
    2.2.5 Propensity to trust ............................................................................................... 14
  2.3 Security in mobile banking ............................................................................................ 14
    2.3.1 Security Mechanisms ........................................................................................... 15
    2.3.2 Perceived security ............................................................................................... 17
  2.4 Determinants of the constructs ...................................................................................... 17
  2.5 Review of similar studies ............................................................................................... 21

Chapter 3: Scientific Method ............................................................................................... 23
  3.1 Choice of topic and preconceptions .............................................................................. 23
  3.2 Research Philosophy .................................................................................................... 24
    3.2.1 Ontological Assumptions: Subjectivism ............................................................... 24
    3.2.2 Epistemological assumptions: Interpretivism ....................................................... 25
    3.2.3 Axiological assumptions: Value bound ............................................................... 25
  3.3 Research Approach: Induction ..................................................................................... 26
  3.4 Research Design: Qualitative ....................................................................................... 27
  3.5 Research purpose: Exploratory ..................................................................................... 27
  3.5 Research Strategy: Case study ..................................................................................... 28
  3.7 Literature Use and scrutiny ........................................................................................... 29
    3.8 Summary of the methodological framework ............................................................. 29

Chapter 4: Practical method .............................................................................................. 31
  4.1 Pilot Study ..................................................................................................................... 31
  4.2 Data Collection ............................................................................................................. 31
  4.3 Sample selection ......................................................................................................... 33
  4.4 Interviewing process ..................................................................................................... 35
  4.5 Transcribing and analysing the data ............................................................................ 36
Chapter 5: Findings........................................................................................................... 37
  5.1 General Attitudes and perceptions ........................................................................... 37
  5.2 Trust in mobile banking .......................................................................................... 37
  5.2.1: Institution based trust ...................................................................................... 37
  5.2.2: Users’ propensity to trust ................................................................................ 39
  5.2.3 Trust in technology .......................................................................................... 40
  5.4 Application Quality ............................................................................................... 41
  5.5 Visible security mechanisms .................................................................................. 43
  5.6 User experience ..................................................................................................... 45
  5.7 Amount of transfer ................................................................................................ 46
  5.8 Device .................................................................................................................... 47
  5.9 Network and connectivity ...................................................................................... 48
  5.10 Other concerns ..................................................................................................... 49
  5.11 Familiarity ............................................................................................................ 49
  5.12 Level of awareness ............................................................................................... 49
  5.13 Users suggestions to improve security ................................................................. 50

Chapter 6: Analysis and discussion ............................................................................... 51
  6.1 Users Trust in Mobile banking ............................................................................... 51
   6.1.1 Institution-based trust ...................................................................................... 51
   6.1.2 Propensity to trust ......................................................................................... 52
   6.1.3 Trust in technology ....................................................................................... 52
  6.2 Application Quality ............................................................................................... 53
   6.2.1 Usage experience ........................................................................................... 54
   6.2.2 Amount of transfer ......................................................................................... 54
   6.2.3 Device ............................................................................................................. 55
   6.2.4 Network and connectivity ............................................................................... 55
   6.2.5 Familiarity ...................................................................................................... 55
   6.2.6 Awareness of security threats ......................................................................... 56

Chapter 7: Conclusion ..................................................................................................... 58
  7.1 Summary of results and analysis: ........................................................................... 58
  7.2 Main contributions ................................................................................................. 59
  7.3 Limitations of the study ....................................................................................... 59
  7.4 Truth criteria ......................................................................................................... 60
    7.4.1 Reliability ...................................................................................................... 60
    7.4.2 Validity ......................................................................................................... 61
    7.4.3 Generalizability ............................................................................................. 61
  7.5 Future Research .................................................................................................... 62

Chapter 8: Ethical considerations .................................................................................. 63
  8.1 Why research ethics ............................................................................................... 63
  8.2 Before the research ............................................................................................... 63
  8.3 During the research ............................................................................................... 63
  8.4 After the research ................................................................................................ 64

Reference list .................................................................................................................. 66

Appendix ......................................................................................................................... 76
List of Tables
Table 1 Threats caused by Internet attacks ................................................................. 8
Table 2 Security objectives .......................................................................................... 15
Table 3 Assets of smartphones ................................................................................... 17
Table 4 Visible security mechanisms .......................................................................... 18
Table 5 Interview design .............................................................................................. 33
Table 6 Details of all interviewees ............................................................................... 35
Table 7 Theories checked ............................................................................................ 56

List of Figures
Figure 1: Scenario of customer connection to internet. Adapted and modified from (Hutchinson & Warren 2003) .................................................................................. 15
Figure 2 Summary of methodological choices ............................................................ 30
Figure 3 The notice of finding potential interviewees. ............................................... 35
Chapter 1. Introduction

The introductory chapter will provide the reader with a general background of this thesis. It will motivate our choice of the subject in terms of discussing security perceptions and trust for mobile banking young users. Furthermore, the purpose of the study, research questions and objectives of the study will be introduced.

1.1 Background

1.1.1 Mobile banking technology

The time that technology had a major impact in helping banks to improve their services to their customers was with the introduction of the Internet banking. Internet Banking helped give the customer's anytime access to their banks. Customers could check out their account details, get their bank statements, perform transactions like transferring money to other accounts and pay their bills sitting in the comfort of their homes and offices, however the biggest limitation of internet banking is the requirement of a PC with an internet connection, not a big obstacle if we look at the US and the European countries, but definitely a big barrier if we consider most of the developing countries of Asia like China and India. Mobile banking addresses this fundamental limitation of internet banking, as it reduces the customer requirements to just a mobile or a smartphone.

The internet made a significant impact on banks and financial institutions, giving customers access to many banking services around the day at the same time, it made huge cut on banks’ costs. Research suggests that online banking is the cheapest delivery service for many banks. Wireless technology, 3g and 4g networks have enabled banks to offer their customers wider value-added mobile banking services with the ability to access many different banking functions from the mobile phones without geographical and time constraints (Cruz et al., 2010, p.343). It has significantly contributed to the bottom line of many banks, as the average transaction cost for mobile banking is just about one to fifty less than traditional banks (Deloite, 2010, p.4). Banks have been able to expand their market territories, and better understand and meet customer’s banking needs by analysing data collected from customers use of their connected devices. (Palacios & Jun, 2015, p.308)

Mobile banking can be seen as a subset of electronic banking, and is considered as an important distribution and communication channel for retail banking (Pouttschi & Schurig, 2004, p.1) and an extension to internet banking with its own unique characteristics that make it one of the most promising tools in banking services (Laukkanen & Pasanen, 2007, p. 86). Early development of mobile banking was in simple form more than a decade ago. Typically, mobile banking services enabled users to receive information on their account balances via SMS. With the introduction of GPRS network and development of more technologies the services expanded to fund transfers between account, stock trading and confirmation of direct payments via the phone’s browser (Mallat et al., 2004, p. 43), with mobile phones and smartphones becoming very popular and people are spending more average time on mobile devices than desktop computer since 2014, that means people are getting more and more the services available from their computers to their phones that are connected (Chaffey, D. 2017).

There have been studies that found that it has significant advantages to bank customers including cost savings as well as time savings and other benefits (Howcroft et al., 2002, p. 119). Mobile banking enables its customers to access their bank account through mobile devices and smartphones to check their balance, conduct financial transactions. The number of services varies through the mobile and it is expected to increase due to its functionality around the clock with the option to bank virtually anytime and anywhere (Laukkanen & Pasanen, 2007, p. 87). It enables customers access to feature they cannot find online, such as
remote check deposit, person-to-person payments, and it is expected that mobile banking will surpass online banking as the most widely-used banking channel by 2020 with increasing opportunities and potential (Deloitte, 2010, p. 3).

For banks, from an internal aspect, mobile banking contributes to improving financial performance of banks. Banks also believe that because of the convenience and safety of mobile banking, it can provide an efficient and economical developing path to bank system, and will surpass traditional banking from both operational and managerial area (Laforet & Li, 2005, p. 363). To gain competitive advantages, banks should imply such a technical method to remain customers and keep a healthy and lively banking market. At last those competitive advantages will reflect on their financial performance. To be more specific, some practical research also shows that the monthly value of banks and the profitability of banks increase by adopting mobile banking. With the popularization of mobile banking, it is widely acknowledged by banks that mobile banking channel contributes to the reduction of some unnecessary operation cost. (Mutua, 2010, p. 38) For example, transaction fees, it doesn’t involve in manual labour as much as in face-to-face service (Gupta, 2013, p. 3) besides, some infrastructure fees are also avoided. These lead to improving the financial operation of commercial banks.

1.1.2 Younger generations:
Research has highlighted the tendency of younger adults toward adopting new technologies in favour of older ones, a study of 430 young adults between aged 18-24 found that the likelihood towards adoption of new radio and music technologies is high, where users are leaving traditional radio stations for new technologies related to internet (Albarran et al., 2007, p. 92). In mobile banking and internet banking, young customers in particular found to love mobile banking and that the younger generation are keen on this application given the benefits it offers and the prevalence of smartphones among the age group, and they are more predisposed to adopt m-commerce services than any other internet users because these services fit with their lifestyle (Bigne et al., 2005, p. 205). The way in which young people access banking services has seen a huge shift. According to a study made in the UK by Gemalto a digital security provider, more than three quarters of people aged between 25-34 manage their money online, and one in five people have made some kinds of payment using their mobile device, while nearly a quarter use it to check their bank balance. Although mobile and online channels are getting more preferred channels for users to access their banking services, the range of services is important. As smartphones become more versatile, they can play a large role in the interaction between consumers and financial service providers, retailers and other businesses. Given the prevalence of smartphones among younger generations, the mobile banking has the potential to empower consumers and expand access to financial services for underserved populations (Federal reserve, 2016, p. 27).

1.1.3 Trust in mobile banking
The growth in usage of internet banking as well as mobile banking depends upon the generation of costumers’ trust of the medium and technology of banking (Kumra & Mittal, 2004, p. 73) and even nowadays with a large number of subscribers in mobile banking, continuance usage remains a challenge for banks after registration for the service, therefore to increase transactions through this channel customers need to build and maintain trust (Thakur, 2014, p. 628). The concept of trust is not a new concept it is in banking an issue of paramount importance due to the financial risks involved, trust has become even more significant through electronic channels (Kumra & Mittal, 2004, p. 75). Trust has objects that are related to either people organizations, vendors, companies and technologies such as mobile banking that are made by those people (McKnight, 2011, p. 12) each object has its own constructs and dimensions. Banks need to build trust with customers when they use their technologies for the
first time, in order to remove and overcome their perceived risks where the switching cost between channels is low as customers can easily switch to other channels or use other banks, hence it is important for banks to build initial trust (Zhou, 2011, p. 528) in addition to trust building. (Siau & Shen, 2003, p. 93) argue that trust is not one time concept and trust needed to be continued and nurtured as its fragile and can be easily destroyed, and customers need reliability and security to build trust.

One of the biggest challenges facing the online and mobile banking industry is the lack of trust of their customers (Adams et al., 2005, p. 1701) which is an important factor in accelerating the growth of online and mobile applications. Kim & Prabhakar, (2004, p. 1) stated that delayed acceptance of the internet as a retail distribution channel was due to the lack of trust that consumers have in the electronic channels and web merchants. The transactions made on the internet are characterized by uncertainty, anonymity and can occur without any prior human contact or established inter-personal relationships this creates a circumstance for a security threat for the user, which justifies the need for more security in electronic environment (Tsiakis & Sthephanides, 2005, p. 10).

1.1.4 Security in mobile banking

For an online user, security is a highly rated issue in their trust in the online and mobile services (Adams et al., 2005, p. 1710) since customers have to provide their banking details and other personal information when conducting transactions on mobile phones, they perceive internet transactions as less secure (Harris & Goode, 2004, p. 142), while security in internet banking could be better than mobile banking as it offers better security and embedded solutions than the WAP, or 4g mobile banking (Kim, et al., 2009, p.286), the perception of security and risks in customers participation in electronic context of banking and commerce is a key aspect of user participation in that particular channel (Salisbury et al 2001, p.165), hence there are many factors upon which customers assess the security in the channel or medium and base their trust perceptions upon, and the success of an online medium or technology whether in electronic and mobile commerce, is critically affected and based on security because without it the whole system would not work. The security functionality depends on a complex interrelationship between several components including, applications development platforms, databases management systems, software, internet connection, infrastructure and devices used. A weakness in a single component would jeopardize the whole security system (Kesh et al 2002, p. 149), and affect in turn the trust of the customer in the technology used.

1.2 Motivation and knowledge gap

As mobile devices and smartphones have become more involved in our daily lives, with the popularity of these devices explodes the appetite of cybercriminals targeting these devices has grown too. The risk of mobile malware is real and hackers can steal money and sensitive information, manipulate users’ information and even spy on user activities. (Europol, 2016)

There has been many studies covered several concepts of trust in the online banking and internet in general, such studies divided and distinguished trust into several concepts such as (McKnight et al., 1998; McKnight et al., 2002, Pennington et al., 2003; Pavlou & Gefen, 2004; Kim et al., 2009; Lee & Turban, 2001; Bhattacherjee, 2002; Gefen et al., 2003; Kim, 2008; Vance et al., 2008; Sun, 2010; Benamati et al., 2010; Komiak & Benbasat, 2004) these studies have covered the concept of trust that is in human or in people in such as trust in the online vendor, or trust in the bank. Pennington et al. (2003) for example found that trust in the system has proven to be affected by the guarantees and mechanisms of the vendor that will enable successful transactions, while there are other studies that has distinguished trust in people to include trust in technology (Mcknight et al., 2002; Kolsker & Payne, 2008; Corbitt
These studies have examined various determinants and factors that affect trust and trust building customers in different online channels, while on the other hand there have been also studies done around security in the internet and mobile context analysed the technical aspects of online security including several dimensions such as in networks, devices or security threats themselves, these studies include (Kesh et al., 2002; Hutchinson & Warren, 2003; Salisbury et al., 2001; Lubuschagne, 2000; Agarwal et al., 2007; Lewis et al., 2010; Wijland et al., 2016) such studies have provided several outcomes and analysis of security and threats in the online banking contexts and e-commerce in addition to provide the basis and foundation of various security objectives and mechanisms that through which the security of an online channel or tool can be assessed or examined either by professionals or from the perceptions of customers.

It was found that one of the main antecedents of trust and trust building in these contexts is security and its perception from the customers’ side, studies covered security and its relationship with trust include (Salisbury et al., 2001; Suh & Han, 2003; Chellappa & Pavlou, 2004; Belagner et al., 2002; Adams et al., 2005; Linck et al., 2006; Flavian & Guinaliu, 2006; Simpson, et al 2014). Link et al. (2006, p.5) stated the average users do not understand the technical aspects of security, therefore for them they evaluate the security through these subjective perceptions. Suh & Han (2003p.132) explained that trust is examined as the mediating factor of the relationship between security perceptions and technology acceptance of internet banking. They examined therefore the perceptions of security control on technology acceptance of e-commerce. In the context of young users, we found studies covered mainly factors affecting the adoption of the mobile banking technology such as (Lewis et al., 2010; Akturan & Tezcan, 2012; Wijland et al., 2016). Wijland et al.(2016) investigated the engagement of young mobile banking users and the importance of this age group for bank managers to sustain their market shares, while Kim et al.(2010) examined the security and trust perceptions from the customers view point about issues related to electronic payment services emphasizing on that security improves trust, therefore we think that investigating the young users perceptions of security and trust in the context of mobile banking deserves to be studied for our thesis, from the above discussion of previous findings we intend on adding to the stream of literature on technology and banking by examining the security perceptions of mobile banking young users due to their engagement of mobile banking services.

1.3 Problem discussion

Mobile banking identity theft is the major purpose for hackers where they sell user information on dark websites to fraudsters who exploit the information they got to pursue financial gains (Chelsey, 2016). According to the American federal trade commission number the monthly reported incidents of mobile identity thefts has risen by the double between 2013 and 2016 (FTC, 2016). There are various ways fraudsters can obtain access to a mobile banking user identity including planting mobile malware to obtain sensitive information from users, scam e-mails, sim card splitting and many others, so users themselves are the weakest point to hack the systems and structures of mobile banking given that banks are able to protect their servers, and no matter how much of expertise used to be put into securing information systems and providing security mechanisms, most of the vulnerability is from users (Mettouris et al., 2015, p. 273), thus they are more targeted by such attacks. According to (Jeon et al., p. 315) users’ lack of awareness of security threats is one of the main threats to their smartphones security.
The importance of user awareness to security threats and user attention to security has been recognised and identified by the European cybercrime centre that established campaigns to raise the awareness of cybercrime among users, in different languages and among many countries within the EU, however we think that it is not enough and banks themselves need to participate and raise the awareness levels of their customers and educate them on how to protect themselves. This would save them costs of compensating affected users and also help in establishing and maintaining the customers’ levels of trust in banks and the technologies associated with their services. Therefore, we aim to examine how mobile banking young users perceive security and different threats around mobile banking technology.

1.4 Research purpose and question
The purpose of this study is to examine security perceptions of mobile banking young users and its effects on their trust in the technology, and to shed more light on the relationship between awareness of security threats and trust in mobile banking, by examining factors that affect the perceptions of users around different security mechanisms provided by their banks in order to secure their mobile banking applications in addition to examining the relationship between their trust and perception of mobile threats that affect their mobile banking experience. The objective is to provide further knowledge about the subject of security and trust in mobile banking technology and give more insights for the banks who develop application about how would young users perceive their application from security point of view.

This study aims to answer the following question:

*How do young users of mobile banking perceive security and trust in Mobile banking technology?*

1.5 Intended contribution
This thesis contributes to the building of existing relevant literature by covering and increasing the knowledge about the perceptions of security in the area of mobile banking by conducting a qualitative study that covers interviewees of existing users of mobile banking technology to investigate the various opinions of young mobile banking users about the discussed points and provide further information to academics who want to make more studies on this field, hence we aim at providing insights about mobile banking usage experiences of young users, we also want to raise the attention to do further studies around the young users of other technologies not only the ones limited to online or mobile banking but other contexts and fields such as gaming and others, since we believe that the majority of younger people are heavily involved in the use of technology.

In addition to our target of providing theoretical contribution to the literature, we also want to raise the level of interest in the practical field towards the negative aspects of technology and security issues involved in the use of mobile banking, since the popularity of electronic payments and mobile banking is increasing and societies are more headed towards adoption of non-paper based money which will lead to increased amounts of attacks and cybercrime in the next period. By focusing the attention on the customers, we aim to highlight the importance of users being the first line of defence to security threats involved with their online banking transactions.

1.7 Thesis disposition
The thesis is organized as follow with the remaining chapters that will build up to the concluding chapter which provides answers to our posed research questions and aims to close the found gaps. The next chapter is Chapter 2: Theoretical background Will provide a detailed discussion of our selected theories and the literature review, the chapter will discuss
thoroughly the concepts of trust and security that are related to this study in addition to covering the various factors that affect both of them. Chapter 3: Scientific method will delve into the scientific methodology that relates to particular philosophical values that serve as the basis of this study, we describe in this chapter the various assumptions and scientific choices we made adopting them from the “Research onion” framework that describes and highlight many scientific approaches to conduct a research. Chapter 4: Practical method will discuss the practical steps and the conduction of the study in accordance with our scientific choices in order to obtain the information we seek from the participants, the chapter contains information about the background of participants, the interviewing processes and data analysis process we made. Chapter 5: Findings will build on the theoretical background part and in which we list and present our findings. Chapter 6 Analysis and discussion will analyze our findings and connect to the theoretical backgrounds we selected. Chapter 7 Conclusions as indicated it will provide our main contributions and answers to our questions.
Chapter 2: Theoretical background

In this chapter, we present the relevant theories and background of our thesis. We start with providing related definitions and explaining what threats can affect the user of the technology. Later we discuss the concepts of trust and perceived security. Finally, we end the chapter with listing several factors found in the literature to be playing a role in forming such perceptions.

2.1 Related definitions

A definition of mobile banking is a communication channel whereby the customer interacts with a bank he or she uses via a mobile device, such as mobile phone or personal digital assistant, the emphasis is on data communication (Barnes & Corbit, 2003 p. 275). Similarly, Laukkanen and Pasanen (2008, p. 87) define mobile banking as a channel whereby customer interacts with a bank via mobile device, another definition is the use of mobile devices to undertake and perform financial transactions linked to a client’s bank account (Anderson, 2010, p. 18), the latter definition could be more suitable since most of the mobile banking activities are done through smartphones that allow more features.

It is important to distinguish and list different concepts around the banking and financial transactions done by the phones, mobile payments for example refers to making transactions through mobile devices including mobile phones, personal digital assistance and other (Chen 2008, p. 33), while mobile commerce refers to the ability to purchase goods and services anywhere through wireless internet-enabled devices (Clarke 2001, p. 133). SMS banking allows text messages of up to 160 characters to be sent from and to mobile phones through which a customer can interact and request different services from the bank to their accounts (Barnes & Corbit, 2003, p. 277).

2.1.1 Security and mobile banking

As the topic of this thesis is about perceptions of security in mobile banking, it is essential to give certain information of what is meant by mobile banking and other mobile services in general. Mobile services by nature can include mobile phones or other handheld devices such as tablets or personal digital assistants or PDAs. There are many of the services that were previously available only in the computer and online environment and today with the movement towards smartphones it is believed that mobile usage will surpass the computer usage by 2020. The different mobile services can include for example mobile shopping, e-mail, mobile banking and mobile payments in addition to performing social media services. Compared to the computer internet and wired electronic services, mobile banking services are bringing additional values such as flexibility, personalization and location services with the ability to use the services anywhere and anytime.

The nature of security on mobile banking services has not changed fundamentally since their introduction, especially the authentication mechanisms where most of the mobile banking services required users to provide usernames and password, then with the time new authentication mechanisms have been introduced such as digital IDs and biometrics (El khodr et al., 2012, p. 260) which is the use of personal fingerprint for authenticating the owner of the mobile banking account. The speed of advancement of technology and importance of mobile device in conducting mobile banking did not remove all security threats and concerns for users. In addition to user authentication and protection of mobile banking, there is also another security aspect of mobile banking that needs protection which user’s confidential information that is often required in the services by different encryption techniques.

Security has been identified as a factor that potentially affects trust in mobile banking. Many scholars argue that security is an important and key factor in building and developing online
trust where Belagner et al (2002, p. 248) stress on that one of the main factors that assist in developing trust in online users is the assurance of safety and security, including other studies that have examined security and trust relationships such as (Adams et al., 2005; Yousafzai & Pallister, 2003; Suh & Han, 2003; Casalò et al., 2006; Shin et al., 2010). According to these scholars, good security improves trust and perceptions of good security and trust will ultimately increase the use of the service.

Since that the transactions are made through internet such as mobile banking, they are based on the account-holder authentication in a way that they could not be done by without the confirmation of the identity of the account holder, there are four actors who are typically involved in an online transaction these include: the sender, the receiver, the financial institution (the bank in our case), the network provider and the payment service provider if applicable such as using Swish (Agarawal et al., 2007, p.142), the transaction is performed through the mobile transaction provider which involves secure transaction protocols, the same applies for banks who process the transactions on the basis of the identity and authentication of the user (Herzberg, 2007, p. 55)

2.1.2 Threats to mobile banking security
According to Ghosh (2010, p. 9) an ID abuse occurs on the form of ID theft and ID fraud, where hackers attempt to attack, intercept and manipulate personal information, break into insecure systems, and exploiting selling those information on any available functionality. ID theft is the exposure of personal information that happens when a victim’s personal information is used by another individual without permission, while ID fraud is the actual misuse of information for financial gain where fraudsters illegally obtain and make fraudulent purchases or withdrawals, open false account and or attempt to get services on the expense of the victim.

Since that the transactions are made through internet such as mobile banking, they are based on the account-holder authentication in a way that they could not be done by without the confirmation of the identity of the account holder, so the vulnerability of the mobile banking would come from the user’s device who is the sender or the receiver, because usually bank and network provider they have relatively more secure systems (Herzberg, 2007, p. 54). Jeon et al. (2011, p. 316) stressed on the importance of awareness of users to their smartphones and classified threats of smartphone whether if they were caused by attacks or by the user unawareness.

Below we list main threats that could affect a mobile banking user. We classified it into two main categories that may be caused by the internet or lack of awareness of the user.

Table 1 Threats caused by internet attacks

<table>
<thead>
<tr>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>• A malware can alter or expose private information in smartphone, causing abuse for costly services and function by manipulating several functions on the phone.</td>
</tr>
<tr>
<td>Wi-Fi network attack</td>
<td>• An attacker can manipulate and change information on the wireless network.</td>
</tr>
<tr>
<td>Denial of service</td>
<td>• An attacker can attack a base station, wireless network or web server causing interruption of the mobile banking service or lag in a transaction</td>
</tr>
<tr>
<td>Break-in</td>
<td>• An attacker gains partial or full control over the target smartphone by using flaw of code, code injection or simply</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Malfunction</strong></td>
<td>• The user can disable his or her application by mistake or misappropriate configuration such as un-updating an old version of mobile banking application or leaving a connected session of mobile banking without logging out.</td>
</tr>
</tbody>
</table>
| **Phishing**    | • The user exposes his or her private information by accessing phishing site or fake website giving their mobile banking details thinking of them that they are buying from a legitimate website.  
• The user can expose his or her private or mobile banking information by sending texts to unknown 3rd party. |
| **Device Loss**  | • The user loses his or her phone |
| **Platform alteration** | • The user attempts to modify the smartphone platform such as jailbreaking or rooting an IOS software or rooting and android device. |

### 2.2 Trust concepts

In the online banking environment, most of the trust literature has covered the cognitive side of trust which refers to the belief that others will not take advantage of the situation by behaving in opportunist manner but rather will fulfil their expected commitment (Gefen et al., 2004, p. 264) another definition of cognitive trust is that people will choose whom they trust and in what situations and under what circumstances and that they base the choice on what they take good reasons that constitute evidence of trustworthiness (Lewis & Weigert, 1985, p. 970) and according to Komiak & Benbasat (2006, p. 943) cognitive trust can be viewed as a set of beliefs about the trustee’s trustworthiness attributes. Beside the cognitive component of trust, trust has also an affective/emotional side and researchers have mad distinctions between both concepts of trust.

Emotional trust has received less attention in the literature (Komiak & Benbasat, 2004, p. 181) has investigated the emotional trust and proposed a differentiation between the cognitive and emotional trust. It refers to the emotional bonds between trustors and trustees (Lewis & Weiger, 1985, p. 971), where trust involves more than simply cold-blooded rational prediction it often carries an emotional investment that can run as deep as friendship or love (Sun, 2010, p. 185), the same author argues that affective/emotional trust plays important role in trust because it supplements cognitive trust when incomplete information about a trustee or the situation is unavailable, and thus cognitive trust alone is insufficient. In our context, it refers to that the feeling of trust about mobile banking due to lack of information about the security threats hence users have another type of trust which is the affective/emotional side of trust. The affective/emotional trust is defined as the extent to which one feels secure and comfortable about relying on the trustee (Sun, 2010, p. 185).

Trust is said to exist between parties who are involved in a transaction this would comprise that the trustor party who is engaged in receiving the services provided by the trustee parties (McKnight et al., 1998, p. 474) In the banking industry, customers are using the service of mobile banking in doing their financial transactions which makes them the trustors, while the bank and the technology of mobile banking are the trustees in this case, where any lack of trust in one of the trustees would affect the whole transaction. According to McKnight (2011, p. 126) trust has several objects that play the role of the trustee or who the trust falls on, which are: trust in humans and trust in Technology.
Early definitions of human-like trust in the literature go back the eighties, where trust referred to “a generalized expectancy held by a customer that word, promise or statement of the company can be relied upon” (Rempel & Zanna, 1985, p. 95), also trust is defined as the willingness to rely on an exchange partner in whom one has confidence (Moorman et al., 1992, p. 315), also Morgan & Hunt (1994, p. 23) recognize that trust exists when one party has confidence in an exchange partner’s reliability and integrity, in services relationships area. Berry & Parasuraman (1991, p. 139) said that relationships are built on the foundation of commitment, where they found that trust affect both relationship quality and commitment between the costumer and the service provider. It has been difficult to define and measure trust and researchers have called the state of trust definitions a “confusing potpourri” (Shapiro 1987, cited in McKnight et al 2002, p. 335).

Trust is defined as feelings of confidence and security on the part of customers that they can have some assurance that the company will look after them. (Kumra & Mittal 2004 p.77), where in banking trust is an important issue for customers and business relationships due to the financial risks involved, it becomes even more significant when using electronic channels. (Kumra & Mittal 2004, p.77), because it helps consumers over-come uncertainty and risk of engagement in behaviours that are related to trust (McKnight 2002p.335) such with using technologies that are related to online nature where the generation of consumer’s trust in using technologies related to internet such as in mobile banking (Kumra & Mittal 2004, p.77).

2.2.1 Trust in technology
McKnight et al. (2011, p.12) assumes that the influence of trust in people on individual decisions to use technology such as mobile banking is more natural than trusting the technology itself, where people present considerable uncertainty to the trustor because of their volition which something that the technology normally lacks. In our context that is the influence of people on themselves to adopt the technology is stronger than the technology itself, while Friedman et al. (2000, p. 36) stressed on that trust is between people and people not people and technology. Hence McKnight et al. (2011, p.12) conceptualized trust in a technology also means that the trustor is willing to depend on a technology in situations where uncertainty arises in which it may or may not complete a task. In our context, it is the trust in mobile banking technology to perform transactions and banking operations with its use. There are two types of trust related to trust in technology as trust develops when relationships evolve these types are Initial trust and knowledge based trust.

Initial trust is the trust and judgements of the trustor before experience with the trustee (McKnight et al., 1998, p. 473) in which the mobile banking users for instance experience for the first time the technology for using it in mobile transactions. Initial trust is discussed widely in the online trust literature such as trust in Web vendors including (Van der heijden et al., 2003; Lee & Turban, 2001; Bhattacherjee, 2002; McKnight et al., 2002; Gefan et al., 2003; Kim, 2008; Vance et al., 2008:). The other type of trust is knowledge-based trust which means that the trustor knows the other party well enough to predict trustee behaviour in a situation (Lewicki & Bunker, 1996, p. 121) which can be related to our case by the fact that users experienced technology for some time and hence the trust in that technology such in Mobile banking may change or erode quickly when costs and benefits change (McKnight, 2011, p.14) such when users experience issues with security and privacy when they use the Mobile banking transactions.

Knowledge based or continuance trust is still relatively receiving less attention, we mention studies done around the area of knowledge based-trust including (Pavlou, 2003, p. 113) where trust in vendor is based on past transactions and reputation, determines risk perceptions, beliefs and behavioural intentions while Pavlou & Gefen (2004, p. 37) found that trust in a
community of sellers determines transaction intentions and Lippert & Forman (2006) showed that trust in technology solution affects perceptions of supply chain technology and long-term interaction between supply chain partners, and that knowledge trust influences IT and purchase intentions (McKnight et al 2011p. 12:4) the concept of knowledge based trust is similar to continuance trust where Siau & Shen (2003, p.93) stressed that trust building involves initial trust and continuance trust, where trust changes over time (Zahedi & Song, 2008, p.226) and that trust is not a one-time concept that is consumed only once but it evolves and develops over time (Siau & Shen 2003, p.93).

We consider in our study the knowledge-based trust since our interviewees are already using the mobile banking application for some time so we dismiss the initial trust from the study. The difference in trust between the two types of trustees can be categorized into three elements according to McKnight et al (2011, p.12:4) which are contextual condition, object of dependence and nature of trustor’s expectations.

In contextual condition users may experience situations of risk, uncertainty and total lack of control of the technology because they depend on it to complete a task (McKnight 2011 et al., p.12:4), where the user risks that the mobile banking is unable to serve his or her expectations of functioning, due to a condition of uncertainty and security issues, where the user for example when using mobile banking may be exposed to uncertainty related to transmitting data over the internet and storing confidential data on the server or device the user is using (McKnight et al., 2011 p.12:4) in our case the condition of risk where the user may store sensitive information on the application hosted by the bank’s server and also storing the information on the user’s device, such information could be the application credentials used to log in the account, account numbers and other information may be related to the user.

While about the object of dependence the difference is the trustee itself where trust in people one trusts a person while in the case of technology the specific technology that is a human-created artefact with a limited range of capabilities that lacks volition, will and moral agency (McKnight et al., 2011, p.12:5), for example when a user decides to perform a transaction by visiting a local bank brand or use a technology such as the mobile phone and the mobile banking application to perform the transaction over the internet then the user trusts in this case the technology. The nature of trustors’ expectations is that when forming trust in people and technology, people consider different attributes of the object of dependence, where users assess different attributes that reflect their beliefs about the ability of the technology, such beliefs may differ based on their expectation or the context for its use (McKnight et al 2011, p.12:5) where users for example of mobile banking assess the application on different set of the attributes such as its capabilities and security measures.

Trust is a multi-dimensional concept by most researchers, where each dimension must be identified and different researchers have presented a variety of definition to the dimensions and elements of trust according to McKnight (2002, p.337) trust has mainly four dimensions which are: propensity to trust, institution based trust, trusting beliefs and trusting intentions he later applied those dimensions on technology where also trust in a specific technology is composed of those four dimensions.

2.2.2 Institution based trust
Institution-based trust focuses attention on trust across situations, on the belief that success is likely because of supportive situations and structures tied to a specific context or class of technologies (McKnight et al., 2011 p.12:8) in our context it is the belief and perception that the situations and contexts in which the mobile banking is used that is part in the online environments affects this type of trust.
Technological and legal safeguards that produce institution-based trust are important to mobile banking user which has two dimensions: structural assurance and situational normality. Structural assurance means the belief that structures like guarantees, regulations, promises, while structural normality means the beliefs that the environment is in proper order and success is likely because the situation is normal or favourable. (McKnight et al., 2002 p.339), while in technology such as in mobile banking structural assurance is the belief that success with it is likely because regardless of the characteristics of the service, one believes structural conditions like guarantees, contracts support or other safeguards exists in the general type of the technology that make success more likely (McKnight et al., 2011, p.12:7), people understand that there are uncertainties and risks associated with online channels because the information asymmetry within this context (Kim et al., 2009, p.290). The need of formal structural assurances that prevent opportunistic behaviours is crucial to build confidence in the m-commerce context, in mobile banking, for example the promises by the banks to maintain the mobile banking interfaces safe and secure with covering up in case of any potential losses of financial value because of the service faults and the protection of customer information and privacy. According to Gefen et al. (2003, p.51) the belief of strength of security mechanisms built into a website supports the building of online trust in e-commerce, while Pennington et al (2003, p.201) states that the security statements provided by the trustor that contain information about privacy policy and security in the system assures the user and influence positively their trust in the system used. According to Kim et al. (2009, p.290) structural assurance in mobile banking include compensation for financial losses because of service faults and the protection of user information. Similarly, in our context we examine the structural assurance on the level of young consumers who use mobile banking.

Situation normality in technology such as mobile banking is the belief that success with the specific technology is likely because one feels comfortable when one uses the general type of technology of which a specific technology may be an instance (McKnight et al., 2011, p.12:7), in the online environment it is referred to the social presence and its implications on trust. Gefen et al (2003, p.7) found that social presence to be an important factor that affect trust, they argue that the social characteristics of the medium where information is being exchanged such as in e-mail, media channels, websites that transfer information is being insecure to communicate sensitive information and that face to face communication is more fitting to discuss personal matters. We examine in our study the effect of transmitting information sensitive between the bank and the user of mobile banking such as login credentials, credit card PIN codes and other information that is considered sensitive for the user and whether they prefer the face-to-face communication to handle such matters. One of the factors affecting trust is user demographics. Gender, geographical location and culture of the user can affect the perceptions of security and privacy as stated by Shin (2010, p.432).

2.2.3 Trusting beliefs

Trusty beliefs in technology is the third dimension and it implies that trusting beliefs in a specific technology exists at a deeper level than its individual trusting beliefs, and it reflects beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible (McKnight et al., 2011,p.12:7) that is the beliefs about the mobile banking technology has the necessary qualities and attributes to perform and function as expected by the user where the user need to have a protective technology to his banking account and avoid negative issues that might arise from lack of security. Trusting beliefs in mobile banking can be reflected in three beliefs: reliability, functionality and helpfulness.

Reliability is the belief that the specific technology will operate properly, the hopes that the technology is consistent, predictable or reliable, where the user might be in risk of that the
technology may not function consistently due to some flaws or situational events that cause failures (McKnight 2011, p.12:6, reliability was found an important factor influencing initial trust in e-commerce (Kim & Prabhakar, 2004, p.1). In our context, we examine the perceptions of the risk that the mobile banking would stop working due to some technical issues caused by a security breach or attack to the bank system or attacks to smartphone or the application itself that might cause the device or the application to stop functioning.

Functionality is the belief that the specific technology has the capability, functions or features to do for one what one needs to be done (McKnight 2011, p.12:5) which indicates in our case that the mobile banking technology is capable to perform as the user expected it to do, (Thatcher et al., 2011, p. 58) stress on that a lack of trust in the technology may cause the users to believe that the technology lacks functionality which leads them to stop using it or explore new applications. We examine users when they consider whether the mobile banking technology delivers the functionality promised by providing features sets needed to complete a task and performing transactions or other activities involve the use of mobile banking. Helpfulness is the belief that the specific technology provides adequate and responsive help for users (McKnight et al., 2011, p.12:2). In our context, the degree to which a user trusts the mobile banking technology to operate properly without interruptions and lags, and that the mobile banking technology is capable of functioning according to users’ expectations and that it provides the help for users in specific situations. Similar to trusting beliefs in human however the names differ were beliefs in human were composed of three beliefs that are: ability, integrity and benevolence.

Ability refers to the trustor’s perception of trustee’s competences and knowledge to the expected behaviour (Mayer et al., 1995, p.709), such perceptions may be based on prior experience or institutional endorsements, where in e-commerce for example perceptions of firm’s ability are based on two related beliefs whether if the firm is competent enough to perform the behaviour or has access to the knowledge require to perform the behaviour appropriately, in mobile banking context a bank’s ability is whether a bank can perform enough effort to keep up the security levels high and risk levels low so that users continue to use mobile banking. Integrity refers to trustor’s perception that the trustee will adhere set of principle or rules of exchange acceptable to the trustor during and after the exchange (Mayer et al, 1995, p.709), in mobile banking context it refers to the conduct of online mobile transactions, customer service policies and banks use of private information, for instance how a bank uses the private information of customers to analyse their buying behaviours, and how banks respond and deal in situations where customers banks account get compromised and whether they can restore their customers trust in their services with their customer service policies. Benevolence is the extent to which a trustee is believed to intend doing good to the trustor beyond its own profit motive (Mayer et al, p.718) a benevolent trustee would help the trustor even when the trustee is not required to be helpful or is not rewarded for being helpful. Benevolence introduces faith and altruism in a relationship (Bhattacherjee, 2002, p.217) where in mobile banking context the situation which a bank behaves towards different customers they have such as whether they deal differently with their customers or not on the basis of age, profit or repeated purchases, for example if a customer has been compromised and in this case what the bank would do to restore the confidence back regardless of what the bank gets from this customer.

2.2.4 Trusting intentions

Trust intentions are the intentions to engage in trust related behaviours, trusting intentions means the trustor is willing to depend or intends to depend on the trustee-in our case the bank and mobile banking technology. There are two basic intentions for trustors, the first is willingness to depend on the trustee in our context the bank and mobile banking, willingness
to depend is the volitional preparedness to make oneself vulnerable to the trustee in the sense of accepting to be dependent on the trustee, the other intention is the subjective probability of depending which is the perceived likelihood that one will depend on the other, where in this context, Curral and Judge (1995, p.151) define trust behaviour as an intention of oneself to rely on another under a condition of risk, which in this case the acceptance and consent of a user to share information with other person, on the web a consumer would be willing to depend if they agree to general statements about volitional preparedness to rely on the vendor(McKnight et al., 2002, p.337) in mobile banking a person would agree to share information and usage history of browsing and shopping related data when they agree on general statements with their banks, consumer subjective probability of depending involves the projected intention to engage in three specific risky behaviours-provide the vendor personal information like providing banks personal information, engage in a purchase transaction, or act on vendor information such as financial advice.(Mcknight et al., 2002, p.337). In our-context we find the user of mobile banking engages in those three risky behaviours in a way that the user agrees on sharing they data of mobile usage with the bank, engage in purchase transactions where they shop online using their mobile devices and act on vendor information such as loan offers and stock advices available in the mobile banking application provided by the bank.

2.2.5 Propensity to trust
Propensity to trust refers to the general tendency to be willing to depend on a technology across a broad spectrum of situations and technologies (McKnight et al., 2011, p.12:7) where propensity refers to that trust is dynamic trait not a stable and unchangeable (Mayer et al., 1995 p. 714) it is neither trustee specific nor situation specific. In our context, we refer to it as the general tendency to be dependent on the mobile banking technology across different situations and contexts such as when users travel and change environments, mobile devices or internet connections.

Propensity to trust is composed mainly of two constructs: faith in general technology and trusting stance. Faith in general technology refers to individuals’ beliefs about attributes of information technologies in general (McKnight et al., 2011, p.12:6) for example one assumes information provided by the mobile banking application is reliable, functional and provides necessary help to perform a task. While trusting stance in general technology refers to the degree to which users believe that positive outcomes will result from relying on technology (McKnight 2011., p.12:6) in our case the degree to which users will believe that positive experience will result from using the mobile banking application and that it will save them effort and time in performing banking transactions anytime and anywhere with their mobile phone. When one has higher trusting stance one is likely to keep trusting the technology until provided a reason not to (McKnight 2011, p.12:6) which can indicate in our case that users will continue trusting the mobile banking application and technology until something happens and removes that trust such as when a security threat affects their accounts or loss of their private information which may lead to decrease in their trusting stance in using the technology.

2.3 Security in mobile banking
Security is a complex concept, have different definitions by several researchers using diverse classification techniques, generally it is defined as the protection against security threats. In e-commerce, a definition of a threat is an event that can destroy, modify, waste, deny or disclose information or reduce efficiency of the data and network resources (Belanger et al., 2002 p.249). Linck et al. (2006, p.5) divided security into subjective security and objective security. Objective security refers to the technical attributes of the security and it concerns the
technical aspects that ensure integrity, confidentiality, authentication, authorisation, non-repudiation, privacy and auditability. In our context, we measure different security threats that can affect the security perception of mobile banking and trust in the service provided by banks.

2.3.1 Security Mechanisms
Security is primarily composed of a set of security objectives that aim to protect users and systems against threats Hutchinson & Warren (2003, p.68) suggested that there are security requirements which are listed below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Communications between parties involved in mobile banking are restricted to parties involved in the transactions (Suh &amp; Han 2003, p.136).</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data transmitted are not interrupted, created, altered or deleted (Suh &amp; Han 2003, p.136).</td>
</tr>
<tr>
<td>Availability</td>
<td>The ability to provide an uninterrupted service, the mobile banking should be available and working as long as it is connected to internet. (Hutchinson and Warren 2003, p.68)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Ensures that the trading parties in an electronic transaction or communication are who they claim to be. (Suh &amp; Han 2003, p.136)</td>
</tr>
<tr>
<td>Authorization</td>
<td>Making sure that only the user can access the account and authorize payments and transactions made through the mobile phone (Hutchinson &amp; Warren 2003, p.68)</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Involved parties should not be allowed to cancel or deny a transaction after that it’s been made (Suh &amp; Han 2003, p.136)</td>
</tr>
<tr>
<td>Privacy</td>
<td>Personal information about customers collected from their mobile banking transactions is protected from disclosure without approval from the user (Suh &amp; Han 2003, p.136)</td>
</tr>
<tr>
<td>Auditability</td>
<td>The ability to keep an accurate record of all transactions for reconciliation purposes made by the mobile banking (Hutchinson &amp; Warren 2003, p.68)</td>
</tr>
</tbody>
</table>

According to Hutchinson & Warren (2003, p.68) a mobile banking transaction involves typically three areas of security: the internet, the bank and the user’s device. The transaction is broken down to a series of five steps or actions and could be broken down to more actions if necessary, these actions are:

- Action 1: a customer connects to internet network whether its 3g, 4g or Wi-Fi and connects to his or her bank account.
- Action 2: The customer then may use the banking application to perform a transaction, browse the internet looking for goods or services to buy or pay for an invoice for shopping or whatever item bought. Then user initiates and authorizes the transaction from his or her device.
- Action 3: The bank checks if the transaction is executable by verifying if the customer has enough funds available.
- Action 4: Upon completing the transaction a confirmation is sent to the user.
- Action 5: The bank performs and approves the payment recording the transaction and proofing that the transaction is made.

Figure 1: Scenario of customer connection to internet. Adapted and modified from (Hutchinson & Warren 2003)
To analyse each of these steps, the security objectives we defined above can be mapped to security needs and requirements for user activities. For action 1 the user should be able to connect to an internet network from his or her smartphone in any suitable period of time, hence triggering the need for the availability objective. Action 2 requires the user to access his account or provide his or her approval for a transaction to be made and making any changes to account-relevant information triggering in this case the need to authorize and authenticate. Actions 3 and 4 involve communication between the bank and the user hence it triggers confidentiality, privacy and integrity with the user, while the last action that involves keeping track and record of the transaction after it has been made which triggers non-repudiation and auditability. With all these actions and steps the mobile banking user and bank customer must be ensured that the transaction requests made by him would be followed through by the bank, in a way that the bank checks as well and notify the user about confirmation of the transaction.

Since many of young consumers use smartphones today with the increasing importance of them, smartphones are the mobile devices used in the mobile banking transactions. A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a basic phone, it allows to perform most of e-banking transactions and it can be considered as a small computer, where smartphone user can develop and install any program which can be customized according to their special needs. Since smartphone is the device used in mobile banking the threat it is subject to can pose almost the same threat to mobile banking user. (Jeon et al., 2011) analyses the smartphone security and its threats, and suggests counter measures for this device, according to Jeon et al (2003, p.312) there are several environments to which a smartphone is connected that can represent sources of possible technical threats. These environments can represent sources and target of an attack these environments are: the internet network including Wi-Fi and cellular connection; a computer that the smartphone connects to; Bluetooth connection with other device; GPS connection to the satellite. We consider the internet mainly in our paper, so what can be attacked in a smartphone is set of assets that are targeted by the attacker in order to obtain these assets smartphones have three basic assets under which potential targets for attack can be classified. These assets are Private Information, Device assets, Applications (Jeon et al., 2011, p.313).
Information in smartphone can be defined as an asset of smartphone (Jeon et al., 2011, p.313) The information includes all the data user can save and store in smartphone and can be transmitted out of the smartphone, such information may include bank account numbers, saved username and passwords, invoices, private pictures, SMS messages, media files and so on forth. This information is stored by the applications of smartphone, hence the security of smartphone is vital for mobile banking and account safety, then the smartphone itself can be considered as an asset, as it connects to Wi-Fi network hence someone who steals the smartphone can obtain a device connected to an mobile banking account combined with a stolen or pre-hacked information then the stealer can get access to the account, performs transactions and cause losses for the original user (Jeon et al., 2011, p.313), additionally applications on smartphone can be considered an assets as well, such as WhatsApp; e-mail applications; text files applications (word and notebooks), such applications may contain information about their banking account.

2.3.2 Perceived security
The perception of security is defined as the subjective probability with which consumers believe that their personal information will not be viewed, stored, interrupted or manipulated during transit or storage by inappropriate parties (Chellappa & Pavlou., 2002, p.359), while Kolsaker & Payne (2002, p.208) argue that perception is as important as reality, Linck et al. (2008, p.5) defines also subjective security as the degree of the perceived sensation of the procedures of security from the viewpoint of the customer. Perceived security in a website refers to the extent to which one believes that the technology through which transmitting sensitive information is secure (Salisbury et al., 2001, p.166).

2.4 Determinants of the constructs
Application Quality
One of the important factors in building trust is website quality. According to Corbitt et al. (2003, p.205) the appearances, functionality and service quality performed by a website are a direct result of many efforts and strategies therefore, website quality is important for web sites to gain competitive advantages over other competitors (Barnes & Vidgen, 2000, p.2) also McKnight et al (2002, p.341) state that good website quality provides users with strong first impressions which helps in forming the initial trust. The term originates from the definition of information quality referred to information as the message in a communication system (Shannon & Weaver 1949). The information quality is determined by several characteristics or items that reflect the quality of information including: reliability, completeness, volume, format and relevance, in addition security of data, language, convenience of access, utility and understanding (Barnes & Vidgen, 2000, p.3). Vijayasarathy (2004, p.757) states that poorly designed interfaces, cluttered pages and layouts with poor information quality contributes to
customer frustration in mobile banking, we examine the quality of the application provided by banks and the users perceptions of it on several items from the included above.

**Visible security mechanisms**

Perceived security was rated to be highly important for users of mobile banking system. According to Chellappa & Pavlou (2003, p.361), the mechanisms that serve as antecedents to this belief are built upon the self-assessment of various objective technological solutions, this can give users the confidence to interact with their bank account and conduct transactions from the smartphone through mobile banking or can encourage them to do so (Suh & Han, 2003, p.139), hence customer perceptions on the internet of security is influenced by mechanisms of encryption, protection verification and authentication. Encryption is the process of translating information from its original form into an encoded incomprehensible form, a combination of complex mathematical algorithms and keys, this process is implemented through the encryption of several communication channels between banks and users, like providing secure portals and pages where consumers provide their banking information, also within the application itself where users need to provide their information safely.

Protection is the process through which customers are satisfied with the fact that their personal information is being protected by the entity collecting information (Chellappa & Pavlou, 2003, p.361), it is primarily concerned with intrusions at the point or storage or destination, for an mobile banking his or her information could be stored with three main parties, the user him or her-self, the bank and the internet (Hutchinson & Warren, 2003, p.68), from the bank’s side the information collected and gathered by the bank through monitoring the activities and behaviour of the user, while from the internet by providing secure payment protocols and ensuring the safety of data collected at their databases, while for the user it involves the protection on his or her smartphone.

Verification and authentication related to the identity associated with a transaction, where verifying from the user’s identity is the main difference between electronic and traditional transaction (Chellappa & Pavlou, 2003, p.361), the user is required to identify him or herself before logging on to his mobile banking account through various ways that differ from bank to bank, where some banks use user names and passwords, Two-factor authentication, Digital IDs in addition to another verification step to confirm a transaction depends on certain banks. (Adams et al., 2005, p.1701) state that users when use fixed passwords and usernames for a long time are significantly more concerned with the security of their connection.

Banks’ systems do not distinguish among users once they entered matching id credentials, hence an identity fraud crime on mobile banking would not be recognizable by the system where in most countries, credit card purchasing, ATM withdrawals and electronically generated money including mobile banking must be cancelled if users claim not to have authorized them and that they were subjected to fraud (Herzberg, 2007, p.54-55), hence verifications are subject to be manipulated and not always secure.

**Table 4 Visible security mechanisms**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Examples of mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>• Encrypted connections with banks.</td>
</tr>
<tr>
<td></td>
<td>• Warning messages when moving to unsecured network connections.</td>
</tr>
<tr>
<td></td>
<td>• Encrypted connection like SSL</td>
</tr>
<tr>
<td></td>
<td>• Locking/Unlocking credit cards</td>
</tr>
<tr>
<td>Integrity</td>
<td>• Warning/Errors messages</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Availability</td>
<td>• Reduced system Down-time</td>
</tr>
<tr>
<td>Authorization</td>
<td>• PIN code generator</td>
</tr>
<tr>
<td></td>
<td>• Digital IDs</td>
</tr>
<tr>
<td>Authentication</td>
<td>• Login usernames &amp; Passwords</td>
</tr>
<tr>
<td></td>
<td>• Digital IDs</td>
</tr>
<tr>
<td></td>
<td>• Biometrics</td>
</tr>
<tr>
<td></td>
<td>• PIN code generator</td>
</tr>
<tr>
<td>Privacy</td>
<td>• Privacy policies</td>
</tr>
<tr>
<td></td>
<td>• Data collection practises disclosure</td>
</tr>
</tbody>
</table>

**User experience**

Perceived security is determined by user’s subjective evaluation of the service. Therefore, the experience of the user of the mobile banking service is also considered as determinant of the perception of security, however the connection between the usage experience and perceived security is not discussed in the literature although logically a connection may exist. Therefore, we decided to discuss this concept further below.

For a period of time studies, have been conducted in the usability field by several researchers. Increasingly the concept of user experience has gained more interest. It is defined and associated with a variety of meanings ranging from traditional usability to beauty, hedonic affective or experiential aspects of technology use (Hassenzahl et al., 2006 p.91). Despite that user experience has been studied for fairly long time, common agreement of the definition has been achieved to some extent as researchers still have different approaches to the topic (Law et al., 2009, p.719), yet it is still difficult to point out that people when they talk about user experience are referring to one definition or meaning of it.

One of the definition of user experiences is presented in the standard definition of user experience (ISO 9241-219: 2010) is a person’s perceptions and responses resulting from the use and or anticipated use of a product, system or a service. This definition does not give detailed information of what user experience really is, however more attempts have been made to discuss the term of user experience for example (Hassenzahl, 2008, p.12) defined the concept as momentary, primarily evaluative feeling that is either good or bad while interacting with a product or service while Garret (2010) argues that user experience is about how a service works on the outside when someone comes in contact with. In our context, we want to see how the experience of the user can affect the perception of security and trust of the mobile banking user.

**Type of connection**

Users became increasingly concerned about the safety of the information transmitted over a wireless network as the degree of communication of sensitive information like in the case of mobile banking increases (Coursaris & Hassanein, 2002, p.12) while in other cases where information is not sensitive for the user with less personal and interactive services does not bother or concern users. In mobile banking context, it refers to the use of mobile banking application in different types of networks and exchanging sensitive information related to the mobile banking such as communicating with the bank by e-mail. We examine whether there is different perceptions of security or feelings of worry when it comes to connection to public wireless networks. Jeon et al (2011, p.314) state that the wireless network is vulnerable to
several attacks that affect the smartphone by corrupting or modifying information on the wireless network. There is evidence that wireless networks are less secure than wired network (Zafft & Agu, 2012, p.1038), however in our context there may be a difference in the perception of users between both cellular data and wireless networks where users may feel a difference when they are connected to each of the mentioned networks.

**Familiarity**

According to Siau & Shen (2003, p.93) trust is not one-time concept and it needs to be maintained over time, so formation of trust builds on knowledge and familiarity and therefore it requires time to build up. (Gefen, 2000, p.726) suggested that familiarity builds on people’s disposition to trust. Familiarity refers to an understanding that is often based on previous interaction experiences and learning of what, why, where and when other do what they want to do (Luhmann, 1982 cited in Gefen 2000, p.726), it deals with understanding of the current actions of other people or of object according to the same author. Due to uncertainty, people draw on each other’s subjective evaluation and belief that influences their behaviour (Chai & Pavlou 2002, p.240), also Kim et al (2008, p.552) found that a customers’ familiarity with a vendor increases their purchase intention of that vendor. In mobile banking people may relate to the experience and knowledge of their family, acquaintances or friends to form the beliefs and remove their uncertainty about the technology. We examine the level of familiarity and perceptions of security related to it after experiencing the mobile banking application and before experiencing it and how users felt in this regard.

**Type of device**

Coursaris & Hassanein (2002, p.7) stated that security mechanisms in mobile devices can alter and cause security concerns as data is being transferred over mobile network, in addition to bigger opportunity for abuse and misuse due to the nature of the mobile device (Varadharjan, 2000, p.200). It has been mentioned that mobile by nature are vulnerable to more security threats than computers who are exist in stable environment. The type of mobile phone can differ in terms of security for example Apple IOS devices can be more secure than Android devices due to the fact the software is more closed in Apple application store rather than Android software who is more open in general for various developers with less security controls. In general, mobile devices and smartphones store an increasing amount of sensitive data and allow access for many services and applications that were available on the computers (Botha et al 2009 p.130). We examine the perceptions of security related to the type and nature of mobile device whether there are preferences towards specific mobile phones or tendencies to manipulate and change the software of the phone used and how that affects trust and security perceptions of mobile banking users.

**Amount of transfer**

Goeke & Pousttchi (2010p.100) argue that amount of payment does not generally have influence on perceived security, and neither to general security aspects such as privacy. However, the monetary amount when making transaction on mobile banking can have impact on perceived security. Bauer et al. (2005b, p.216) stress that transaction security is major concern for users in e-commerce, where users prefer easy and fast processing for smaller amount and are willing to accept a lower level of security. Also, Mallat et al. (2004, p.46) stated that mobile payments must become faster, easier and more convenient to use where users also prefer simple security mechanisms instead of complex slower procedures. In our context, we examine the amount of money our users put in their bank account that are connected to mobile banking service and the amount of money they perform on transaction and whether it affects their perceptions of security.
Awareness of security threats:

According to Komiak & Benbasat (2004, p.188) awareness has an impact on trust, where given total knowledge there is no need to trust while total ignorance gives no basis to build upon a rational trust. Hence a mobile banking users’ knowledge about a trustee such as the mobile banking technology serves as a foundation for trust formation. Awareness is divided into awareness of known and awareness of unknown. Awareness of known may have a direct relationship with emotional trust or indirect on through cognitive trust by a customer interpretation of his or her knowledge into a rational expectation of a trustee. In our case the interpretations of users about their level of knowledge in technology security mechanisms and threats will have an impact on their cognitive trust. For example, a user may fell less trustful about the mobile banking as they know more about how possibly they might get hacked and hence they might act more carefully in situations where they are more vulnerable to these kinds of threats.

The awareness level of the user about security threats is one of the vulnerabilities to the device (Jeon et al., p. 314). This causes the user to make errors that compromise his mobile banking security as human errors continue to be a major concern in the face of developing the service of mobile banking despite the advances of technology protections and security (Zhang et al., 2009, p.338). Lack of security information has been found to make users poorly aware about security and this may cause users to decrease their perceptions of control and trust in the service and data (Adams et al 2005, p.1704) despite the advances in internet and security technology the fact that customers do not adequately understand security controls make them wary about the security in the technology the hence the actual strength of security controls may not fully be exploited or appreciated by the user (Suh & Han, 2003 p.137).

Awareness of the unknown on the hand will influence both cognitive trust and emotional trust, where emotional trust will decrease due to his or her awareness of the unknown (Komiak & Benbasat, 2004, p.188) for example unknown security threats will affect emotional trust when a user knows about security incidents to mobile banking such as losing money through the news or internet but without knowing how it happened exactly may affect his or her emotional trust in a negative way. Komiak & Benbasat (2004, p.188) found the relationship between awareness and trust, however they stressed on that the relationship with trust can either be positive or negative depending on the context.

2.5 Review of similar studies

After defining and reviewing the concepts of trust and security we now analyse the inter-relationship between them and develop out conceptual model of the covered areas of our study. Security has been identified as a factor that affects trust in a mobile banking user so we try to develop an understanding and between the constructs of trust and security. Security and trust are both defined as multidimensional concepts that are changing as transactions expand from physical world to the electronic world (Yousafzai et al., 2005 p.182), where it was found that perceived security and perceived privacy are two main antecedents of consumer trust in electronic banking(Yousafzai et al., 2003, p.847), while perceived security was also found to influence trust in electronic banking as well(Yap et al., 2010, p.27), in addition to many other studies that found security as an antecedent to trust, fewer studies examined both constructs and the nature of relationship between them including, (Belagner et al., 2002; Suh & Han, 2003; Karnouskos et al., 2004; Adams et al., 2005; Casalo et al., 2007; Agrawal et al., 2014)
(Belagner et al., 2002) investigated the role of privacy, security and site attributes in trustworthiness in e-commerce by studying the relative importance when purchasing goods and services over the web, and found that consumer rating of trustworthiness of web merchants based on four trust indices and that security features are the most significant aspect of trust, they also found that consumers rely on their perception of trustworthiness.

(Suh & Han, 2003) studied the impact of customer trust and perception of security control on the acceptance of electronic commerce, where they examined trust as the mediating factor of the relationship using internet banking as the research domain. The study measured the perception of security and privacy protection in this context as customers are generally concerned about sensitive information such as their financial information using security issues in e-commerce context and trust in e-commerce environment to develop their conceptual model about the perceived strength of security control, findings indicate that privacy protection, data integrity, and nonrepudiation perceptions have significant impact on trust, and that trust also has a significant impact on e-commerce acceptance.

Karnouskos et al (2004) examined the role of security, trust and privacy relevant to related issues in mobile payments where they tested those theories in the m-payment context, focusing on how the security, trust and privacy are tackled in the business model of an M-payment service, they concluded that the security has to be presented in both the business model and the technology used to implement the service since the first day of its implementation.

Adams, et al. (2005) studied the impact of individual security features on trust, the authentication mechanisms of security and their impact on consumer trust and the types of authentication mechanisms that contribute to building trust are examined. The findings indicate that authentication features have an impact on perceived control, awareness and trust in e-banking consumers. Two main authentication types were identified, fixed passwords and security boxes, security boxes are randomly generated passwords that oppose the fixed ones. The results were triangulated from in-depth interviews and questionnaires to compare the different authentication processes, the security boxes and fixed passwords were perceived significantly more trustworthy and secure at any location that the fixed passwords.

Casalo et al (2006) investigated the role of security, privacy, usability and reputation in the development of online banking, describing the positive effects of security and privacy on consumer trust in a website. They suggested that trust has a positive effect on consumer commitment. The study was conducted using structural modelling and compared their proposed model with a rival one. The findings indicate that web site security privacy have significant effect on consumer trust in a financial services website and that consumer trust is positively related to relationship commitment.

Kim et al (2010) studied customers perceptions of security and trust in electronic payment systems as they have become a major factor in the evolution of electronic commerce, their study examined issues related to electronic payment security from the viewpoint of customers finding that technical protections and security statements are significant factors for improving consumers’ perceived security and that perceived security is positively related to consumers’ perceived trust.

Agrawal et al. (2014) investigated the area of distrust on mobile banking, due to number of issues and challenges mainly security issues and concerns by analysing the mobile banking security scope and proposed an authentication system that can be used in mobile banking which is biometric authentication by a new technique which is face authentication for mobile banking services.
Chapter 3: Scientific Method

In this chapter, we discuss and provide a description concerning the scientific methodology used in this study. We begin with discussing the choice of topic. It moves from research philosophy and choices of ontological, epistemological and axiological issues and followed by the approach, design and strategic choice. We also argue our viewpoints in terms of philosophical stances where it logically continues leading the reader to choose of adopting a qualitative approach. Moreover, the chapter discusses issues related to literature search and its procedures to end with our ethical and social considerations of the study.

3.1 Choice of topic and preconceptions

When we first started to think about the thesis, we were thinking about a topic related to technology as we were influenced about the mobile technology due to some courses about information technology we previously had, in addition to general knowledge and interest about mobile & smartphones. We selected the mobile banking to be the object of the study due to its increasing importance and the amount of money is being digitalized nowadays. These elements have motivated us to gain deeper knowledge and understanding about this technology and its uses, how the future of will be and so on forth. When reading about the topic of mobile banking we found that there is decent amount of news online about security threats related to this technology recently which motivated us to select security as we have seen that many users of the technology share one thing in common that is they are not aware of threats and how hackers can actually use their information to access the device.

There have been many incidents related to the security of mobile banking from gathering small bits of information to full identity frauds. Users are leaving huge amount of data every day from their social media uses and extensive use of the internet which make them more vulnerable to internet and mobile attacks especially with the rise of smartphones and that they become almost same as computers in terms of security threats and hacking problems, therefore we aimed at highlighting this topic in the research field and contribute to the current literature. In reviewing which, we identified a worthwhile relation between the concept of trust and security in several fields and technologies especially in the banking industry as users need to trust the banks on their money, they need to trust their technologies as well. Security of the technology is vital for banks to build and maintain trust levels of their users in order for them to use the technology with minimal worries about security threats. We chose he younger students as our domain of search and scope of participants because we believe that they are the most demographic group of people who use technologies in general and mobile banking and payments in particular, they rely on smartphones in almost every aspect of their life: in communication, social media, banking, and other applications which requires them to be connected and updated around the clock.

To our knowledge the subject we study is not widely covered, most of the studies focused on the concept of trust and factors affecting it including security, but fewer studies were done to know in depth perceptions of security from young users’ point of view, thus this gives an opportunity for us to explore further in the area and move more from general studies to in-depth studies to examine younger users’ perceptions of mobile banking technology security. We found that our location can be very suitable since we are: first in Europe in which it applies widely mobile banking technologies and especially in Sweden. Second, our situation as students in Umeå University and the environment around us gave us the possibility to conduct our study.

Moreover, we note that the study results can be subjective since we may interpret them according to some bias we have to form an understandable idea and formulate relevant themes for the study. We wanted to clarify this aspect to rule out objectivity in our research as we will
be conducting interviews and not statistical tests. Our results and findings are done with consultation from our supervisor mainly and some feedback from fellow students.

3.2 Research Philosophy
Philosophy is “a set or system of beliefs (stemming from) the study of the fundamental nature of knowledge, reality, and existence (Waite & Hawker, 2009, p. 685). In doing research, it is natural that a researcher should clarify his/her philosophical standpoints that are used in studying the subject matter. For this, the researcher is expected to state the assumption that he/she has chosen due to the impact he/she cause in practice of research. This is supported by Creswell’s (2014, p. 5) argument that in the process of planning the research, it is necessary to show a clear connection between the philosophical worldview, the design of the research, and the method applied on carrying on the research. Meaning, the strategy or research approach should be in a compulsory relationship with the major two philosophical standpoints that are epistemology and ontology (Scott, 2014, p. 30). In addition, McNabb (2002, p. 37) argued that if the standpoints are properly chosen it will establish the framework on which pillars of the research process, which includes research strategy and data collection methods, are pre-set and applied.

3.2.1 Ontological Assumptions: Subjectivism
According to Saunders et al (2012, p. 130), ontology is concerned with nature of reality. This nature is evaluated by the relation between social entities and social actors. To be more specifically, ontology is the philosophy which discusses the independency of social entities towards social actors. It concerns two possible situations, the one is, social entities can exist without any influence of the actors, the others one is, social entities are strongly related to the actors, so the entities cannot exist independently (Bryman & Bell, 2015, p. 32). Thus, two main ontological philosophies are generally defined based on the discussion: objectivism and constructionism. Objectivism states the existence of social entities is independent of social actors, while constructionism asserts that social phenomena are derived from the interaction or construction of social actors (Saunders et al., 2012 p. 131).

In this sense, the subject for the researcher is that whether she/he wants to realize the phenomena from a deeper perspective, or relationship between certain aspects of it (Ardalan, 2008, p. 3). Here a selection of ontology stance is imminent. If a person seeks for deeper understanding of a situation, it is quite likely to be affected by the subjective approach, whereas, if a person looking for an understanding of the linkage between given aspects, then that takes more external and objective approach (Ardalan, 2008, p. 3). For our thesis subjectivism is the primary ontological assumption that we would argue for as it is essential for answering the research question. As the study is carried on by gathering primary data from qualitative interviews that will be collected from social actors (users of mobile banking), the subject of the researcher the social phenomenon under the subjectivism stance are created from the perceptions and consequent actions of social actors that is a continual process through the process of social interaction, such phenomena are in constant state of revision (Saunders et al 2009, p. 111). Studying the details of the situation to understand the reality or perhaps a reality working behind them is referred to by the term constructionism or social constructionism which derives from the interpretivist philosophy that it is necessary to explore the subjective meanings motivating the actions of social actors in order for researchers to be able to understand these actions (Saunders et al., 2009, p. 111). Social constructionism views reality as being socially constructed. Social actors under study may place many different interpretations on the situation in which they find themselves. In our context of study this can be referred to the mobile banking users under investigation which may have different opinions and interpretations about the security perceptions of the mobile
banking application. Such interpretations are likely to affect their actions and the nature of their social interactions with others (Saunders et al 2009, p.111) in this sense the respondents are not only interacting with their environment but they also seek to make sense of it through their interpretations of events and the meanings that they draw from these events.

3.2.2 Epistemological assumptions: Interpretivism

Epistemology is a philosophy which concerns about acceptable knowledge (Collis and Hussey, 2014, p. 47). The discussion within epistemological philosophy can be mainly interpreted into three levels. In the first place, it argues what is or should be considered acceptable knowledge (Saunders et al., 2012, p. 132). To be more accurate, Bryman and Bell (2015, p. 26) introduced the position of researcher into this philosophy and questioned if the researchers stay out of the knowledge or be a part of it. From a methodological perspective, epistemology views both social science and natural science. It concerns whether they can be studied by similar or relevant research ideas or not (Bryman and Bell, 2015, p. 26).

Generally, there are four main stances existing within epistemological philosophy, they are positivism, realism, interpretivism and pragmatism (Long et al, 2000, p. 191). Positivism is a philosophy which is frequently use by natural scientists. It is based on the existing knowledge and theories or which can be observed and measured, generating relevant hypotheses, and trying to confirm those hypotheses (Saunders et al., 2012, p. 134). Researchers who adopt this philosophy should act as external observers of the knowledge (Bryman and Bell, 2015, p. 26), moreover under the positivist approach the research is taken as far as possible in a value-free way the researcher should be independent and neither affects nor is affected by the subject of the research (Saunders et al., 2009, p.114) this approach of positivism suits in most cases a highly structured and quantifiable observation that lend themselves to statistical analysis which is not what we seek in our study. Realism is quite like positivism, but it gives an answer of the question what is the reality. It states the reality is what people sense, however interpretivism stands in the opposite of the first two approaches where it emphasizes people’s participation when conducting a research. This philosophy recognizes the complication of knowledge where it cannot be simply studied by law-like research method (Bryman and Bell, 2015, p. 28). As social actors, the different roles the researchers play influence their attitudes toward knowledge, which determines that knowledge cannot be completely objective (Saunders et al., 2012, p. 137). The last epistemological philosophy stance is pragmatism. Researchers work with this stance when they conduct a mixed-method study. It claims that when the research question does not clearly imply the possible research philosophy, researchers adopt more than one philosophical position (Saunders et al., 2012, p. 130).

We agree to adopt interpretivism approach to support our study. Our research will be conducted in a qualitative way, according to Collis and Hussey (2014, p. 46) the most proper philosophy assumption applied to qualitative research is interpretivism, particularly, we will collect the necessary data from interviewing people, which mean our research involves in people’s different perspectives and standpoints. Furthermore, we ourselves will also be a part of this research when analysis the data and give conclusion, by taking all these reasons into consideration, we believe that all the respondents and the researchers will participant in the research, which implies us will work with interpretivism as our main epistemological approach.

3.2.3 Axiological assumptions: Value bound

Axiology is the other branch of philosophy that studies judgements about value, although this may include value we possess in fields of aesthetics and ethics. It is the process of social
enquiry with which we are concerned here. The role that our values play in all stages process is of great importance if we wish our research results to be credible (Saunders et al., 2009, p.116). Our values are the guiding reason of all human actions, and researchers who demonstrate axiological skills by being able to articulate their values as basis for making judgements about what research they are conducting and how they go about doing it. After all at all stages of the research process we will demonstrate our own values. According to Saunders et al. (2009, p.116) our choice of philosophical approach is a reflection of our values, as our choice of data collection techniques suggests that we value personal interaction through interviews with our respondents more highly than their views expressed through an anonymous questionnaire, therefore our assumptions of value are bounded since we consider ourselves as a part of what is being researched and cannot be separated so we will be subjective in our data interpretations, unlike if we want to do quantitative where researchers deal with numerical data and have to be objective in their viewpoint and value free from what is being researched.

3.3 Research Approach: Induction
Each research project will be supported by several relevant theories. Research approaches describe the method the researchers choose to connect their observation and the theories they use. The degree the researchers understand and utilize the theories before conducting the investigation contributes to the design of the research project directly (Saunders et al., 2012, p. 143). Research approaches clarify the process of the research, more specifically, they argue which procedure the researchers decide to adopt when they run the analysis in accordance with the theories. Three existing approaches are mostly used in research: deductive, inductive and abductive approaches. Deductive reasoning indicates that the conclusion of the research fully relies on the adopted theories. The researchers draw up the hypotheses when study previous knowledge, and try to test them by using theories (Collis & Hussey, 2014, p. 47-49). Thus, a causal relationship occurs between the conclusion and the theories. We can see deductive approach as from theory to data. When all the premises are right, the outcome will also be right consequently. The second approach, induction, stands in the opposite place of deduction, claims that theories play a part in the further research, but the whole analysis and conclusion will be built on the base of its own situation, realistic investigation. In inductive approach, researches are conducted with a small sample. The research verifies the hypotheses derived from theories and then generates new theories based the verification process, in other words, it is a process from data to theory (Saunders et al., 2012, p. 146). The last approach is abduction. This approach combines both deduction and induction. It starts with the facts the researcher wants to investigate, then maps out a plausible theory to explain these facts (Saunders et al., 2012, p. 147).

Taking the particularity of our theme into account, we believe that induction is the most appropriate approach to direct the research. To understand the nature of the problem, we plan to act interviews to a small number of samples and analyse the data collected by the interview. Saunders et al., 2012, p. 146) More specifically, we are going to gain the knowledge about what is the users’ feeling of mobile banking and how they perceive the security issue of mobile banking through the small sample interview. Based on those data, we can generate the trust issue between banks and their customers, as well as how it effects and how to deal with customer-bank relationships. With the consideration of investigating security issue in certain context of mobile banks and developing new theory about the interaction between customers and banks, we believe the explanation of induction confirms with our basic design of the research. (Saunders et al., 2012, p. 150)
3.4 Research Design: Qualitative

The research strategy is highly depended on the nature of the research questions. (Saunders et al., 2012, p. 161) Since we have already clarified that as an explanatory research, in this paragraph we will continue exploring the most appropriate research methods. Overall, two methods are commonly used in researches, which are qualitative and quantitative research strategy. They are going into different data collection method and analyzing process. The distinctions of them have further affects in following research, so now we will discuss them in detail. Quantitative research often goes with positivism philosophy and deductive approach, where they aim to test theories by data. (Saunders et al., 2012, p. 146) It stresses the utility of quantification data processing method. For instance, quantitative research always adopts numerical variables to examine objective theories. (Saunders et al., 2012, p. 173) This examine process is usually manipulated by statistical techniques. When embrace quantitative research, experimental and survey strategies are mainly linked with the research. (Saunders et al., 2012, p. 174) In contrast, qualitative research method emphasizes social stuff is arising because of relationships and coherences. (David & Sutton, 2011, p. 85) That leads to qualitative research is often associated with interpretive philosophy and inductive approach. (Saunders et al., 2012, p. 174) About data collection and analysis, qualitative research doesn’t have a standardized method to deal with data, if only the procedure is naturalistic and interactive. In qualitative research, researchers tend to emerge the theories after data processing procedure.

From above, we have agreed on following interpretive research philosophy and inductive research approach. Linked to the nature of the research questions, here we decide to adopt qualitative research method in this research. A qualitative research is performing with the goal of investigating the relationship between different elements in the research. (Saunders et al., 2012, p. 174) Those are clearly embedded in our research questions. In our research, we focus on security issue with certain context, mobile banking. In addition, our research questions are motivated by the intension of trying to explain the relationship between them, particularly in customers’ perspective. Taking all this into consideration, we believe qualitative research methods can works adaptively in our research.

3.5 Research purpose: Exploratory

According to Collis and Hussey (2014, p.3) research can be classified based on its purpose, process outcomes and logic. The authors also sub-categorize these items into sub-categories, for example there can be different purposes for conducting a research. The classification of research purposes most often used in the research methods is based on three main purposes which are exploratory, explanatory and descriptive (Saunders et al., 2009, p. 139), we briefly explain and define the three common purposes of studies and chose the one suits our research.

Exploratory studies are often used as means to find out “what is happening” and to seek new insights about assessing phenomenon in a new light. It is particularly useful if the researcher wishes to clarify an understanding of a problem. It can be linked to the activities of the explorer and under an exploratory study, the research can adapt and change the direction as a result of a new data that appear and new insights that occur to the research (Saunders et al., 2009, p.140). Descriptive studies are done to portray an accurate profile of persons, events or situations. It may be an extension to an exploratory research or an explanatory research. It is necessary to have a clear picture of the phenomena on which the researcher wishes to collect the data prior to its collection (Saunders et al., 2009, p.140) while explanatory studies aim to establish relationships between variables. They emphasize on studying a situation or a problem in order to explain the relationships between variables, such studies are mainly done by the analysis of quantitative data (Saunders et al., 2009, p.140).
For this thesis, we think an exploratory purpose suits the most our study as we aim to find new insights about how mobile banking users perceive the security and trust in mobile banking, hence we use qualitative semi-structured interviews.

3.5 Research Strategy: Case study
There are many effective factors which determine the research strategy. The most important are research questions and research objective. Additionally, the research philosophy and approaches we chose, the knowledge holding by researchers, the consumption of time, and other resources we have are also required to be taken into consideration when design the research strategy (Saunders et al., 2009, p. 141). To fulfil a research, we have already suggested literature review and generated research questions from that. But as a full process of a research, we need to continue towards research design, conduct, and analysis (David & Sutton, 2011, p. 102). This indicate that there is an existing relationship between theories, research questions, data collection and display (David & Sutton, 2011, p. 102).

Based on our research questions and philosophy assumptions we made, to secure our data collection method as well as contribute to further analysis, now we need to select suitable research strategy to link those relationships. In fact, there are a variety of strategy choices we have. We point out the distinguishing feature of different strategy, and choose a best fit one. Experimental research is widely applied in natural science study, using to solve the research question about causal relation and the degree the research objectives interact with other factors (Saunders et al., 2009, p. 142). Survey strategy is often related to deductive research approach, answering research questions linked with “who”, “what”, “where”, “how much” and “how many” (Saunders et al., 2009, p. 144). Archival research emphasizes the utility of existing documents and resource. Action research is applied management studies, calls for researching in actions, and the collaboration between researchers and participants (Saunders et al., 2009, p. 147). Grounded theory is used in inductive research, which means it infers theories as its conclusion, on the ground of data interpreting. It is mostly used to predict or explain the behaviour, especially in management and business research (Saunders et al., 2009, p. 149). Case study is a strategy skill when doing empirical research within a present social phenomenon from different sources (Saunders et al., 2009, p. 146-147).

Reviewing above, we have determined our research will be guided by interpretivist philosophy and inductive approach. It is also discussed that explanatory research is more appeal to the nature of our research. Concerning our research questions and objectives, we admit case study strategy will be the most appropriate one in our research. Case study is suitable for explanatory research. It is also able to answer research questions about “why”, “what”, and “how”. Four main genres exist within the context of case study, which is constructed on two dimensions. They are single case and multiple case, holistic case and embedded case (Saunders et al., 2009, p. 146). In our research, we believe if we investigate the whole mobile banking users’ perception, the result must be more precise and convinced. but due to the limitation of time and locations, we will only conduct our research within certain area and special group of people (for instance, divide all residents in one area by their occupation). After that we can start performing a data collection process to address the research questions. Although there are several skills we can adopt, and using different skill with different group of participants is allowed in case study strategy, we will choose interview as our main data collection methods (the data collection techniques will be discussed in detailed in practical method chapter).
3.7 Literature Use and scrutiny

Literature searching process plays an important role in the whole research. This process is performed with the goal of define the utility of relevant literature. According to Collis and Hussey (2014, p 76), by using literature search, the researchers can determine relevant researches outcome in a valid time period. Except that, it can assist the researchers to establish a systemic knowledge system of their study within a certain field. (Saunders et al., 2009, p. 141) The purpose of literature searching is to get a thorough understanding of existing knowledge, basic concepts and theories of this topic, appropriate methods of this topic, critical thinking about this topic, related contributions and so on. (Bryman and Bell, 2015, p. 8) Only by estimate previous studies can we understand the meaning of our research currently, and make contributions to further research.

We now start a literature search to draw a clear map of theoretical foundation. Most of the literature comes from online database like google scholar. In addition, we believe that when formulating methodology part, it requires us holding an objective view of our research, as well as keeping it scientific. With those purposes, we mainly consult scientific books about research methodology in business studies in Umea University library to construct this part. Some of the scientific articles are also as references in this part. Those trustful resources provide us an elaborate knowledge of the basic structure of a thesis, and how to perform a research. In theoretical part, in order to explain the theories supporting the research and the logistical relations between them, we also consult relevant literatures. We do download scientific articles either from Google scholar and Umea University database. Some information from websites also helps us build research background. Books are not used in high frequency in this part because each theory is scattered. When design theoretical framework we try to present them deep enough, so we refer to specific articles of each theory and discuss them in different subheadings. We measure critical thinking of high importance because it offers us not only how the research is conducted but also an overall view in both positive and negative way of the whole research, hence when we proceed in literature search, except consulting literatures which support our viewpoints, we also try to integrate those stand in opposition and explain our choice in this situation.

3.8 Summary of the methodological framework.

In the following figure, we summarize the chapter and show the linkage with the next chapter pertaining to the practical method. Generally, our thesis will adopt interpretivist and subjectivist view which suit the choice of a qualitative design and an exploratory study that the research question could be answered with. Furthermore, the study takes a shape of a case study in fulfilling the requirement of the research question. Overall the study account for classical methodological views that can be found within the field of study.
Figure 2 Summary of methodological choices.
Chapter 4: Practical method

In this chapter, we will continue introduce the methods we adopt in this research. We shed light on the practical method to settle research questions. Data collection method, sample selecting will be presented in this chapter, together with the reasons of choosing them. After those methods, we will go on discuss interview’s conduction, transcription, data analysis method, which will contribute to empirical analysis part. Finally, we focus on reliability and validity, and ethics issues of the research.

4.1 Pilot Study

To get a picture and better understanding of the chosen area of our study, we conducted a pilot study to test how much data we can get before the actual interviews. It is a great way to conduct such studies to make that interview questions are working and sufficient data would be obtained, it would be also good to make sure the whole research is well thought through (Byman, 2008, p.258). Since we wanted to get better understanding about how young users perceive mobile banking security we decided to make a couple of interviews to see how much would people speak about the topic from their point of view. Before collecting the data, we made an interview guide with questions related to our topic and sub questions related to other subthemes we wanted to know about. It is important to understand all the questions relevant to the research topic when collecting the data (Bryman 2008, p. 259). After conducting the pilot interviews the respondents were asked about their background of he discussed topic and how their impression was whether it deserved to be further studied or not, so for us it would mean that we had a reasonable understanding of the chosen area, and to make sure that the questions are easy to understand and answer. Based on the pilot study we modified some of our questions as we thought they were too specific and technical for the respondents and adjusted them to be more open and understandable.

4.2 Data Collection

In methodology chapter, we decided to embrace interpretivism philosophy when designing the research. For the purpose of investigating how social actors interact with each other, we want to gather different opinions from different people. Standing from this point, we believe this research should concentrate on how to collect the data we need in the first place. According to the definition of primary data of Collis and Hussey (2014, p. 130), since we will generate the data from interviews, our primary data collection process should be conducted properly.

Here we have several qualitative data collection methods based on Collis and Hussy (2014, p 133), they are: interviews, focus group, protocol analysis, diary methods and observation. Next, we will give a brief description of them and reason our choice. Interviews are utilized when the researchers aim to hear the thoughts of respondents directly. Those respondents are specifically selected in group of people. Interviews mainly focus on examining their actions, feeling, and thinking by questioning them (Collis & Hussey, 2014, p 133). Focus groups are often used when a prevalent situation happen in a particular group of people. It could be seen as a combination of interview and observation (Collis & Hussey, 2014, p 141). Protocol analysis can be the proper method when the aim of the research is to investigate people’s mental activity in case that they are facing problems (Collis & Hussey, 2014, p 144). Diary method often last over a period, collecting written record of people’s activity, feeling and thinking (Collis & Hussey, 2014, p 146). Observation can be classified into natural observation and artificial observation, with the aim of recording people’s daily actions and behaviour (Collis & Hussey, 2014, p 148). Our research topic is mobile banking and security issue, to address research questions we need to investigate mobile banking users’ comprehension and perception toward this topic. Based on this we believe focus group is not
so suitable because each respondent has their own experiences when using mobile banking, we cannot define a common situation here. Despite that, we decided to preclude protocol analysis due to that in this research we emphasize their feeling rather than the reaction when facing problems. Considering time investing issue, diary method and observations are excluded for the reason that they are too time consuming. Looking back to our research purpose, it is exactly the result what interviews can provide. We want to investigate people’s perception about mobile banking security and trust issues and how it works. By asking them questions in interviews, this purpose can be easily fulfilled. We will generate interview questions through theoretical framework we have built. Assisting by this data collection technique, we are able to set up a bridge through theories to data. In general, we admit interviewing is the most appropriate data collection method in our research. Below we will explain how theory basis contribute to the interviews construction.

Interview can be categorized into two stances. It can be unstructured and semi-structured. Conducting an unstructured interview mean the researchers do not need to decide any predetermined interview questions before the interview. They will organize all the questions when the interview is being conducted. (Collis and Hussey, 2014, p 133) Compared with unstructured interviews, semi-structured interviews require the researchers design some prime questions beforehand, and follow those questions during the interview (Collis and Hussey, 2014, p 133). Open questions are widely used in interviews rather than closed questions in interviews, because we would like to find out people’s feeling and thinking about our topic, we encourage respondents to talk as much as possible. In this research, we choose semi-structured interview as our data collection method. We will discuss what information will be helpful to our research according to research questions and theories basis we established. After figuring that out critical information we need, those will serve as the brief guideline of question designing and interviews.

It is an advantage to use an interview guide when conducting semi-structured interviews to have some guidelines for use during the interview, where we move from one point to another after gathering the necessary information from it. Unlike surveys where usually are more structured and strictly followed, semi-structured interviews allow for additional questions and having a natural flow of conversation with the help of the interview guide (Bryman & Bell, 2011, p. 419) where it is not necessary to follow the interview guide question by question, because in such type of interviews the interviewer is allowed to ask supplementary questions whenever is important under the interpretivist view, which cannot be applied in a quantitative study (Bryman & Bell 2011, p. 419). When conducting semi-structured interviews, asking the right questions can be a challenge, therefore we used our pilot studies as a source of experience for us for this task as it is considered a way for the researcher of practising and developing questioning skills (Bryman & Bell, 2011, p. 422), it also allows to refine the questions so that the respondents have the ease of answering the questions with minimal doubts (Saunders et al., 2009, p. 394).

To collect necessary information from the interviews, the predetermined questions are formulated by different gradations in accordance with the theories basis we discussed in Theoretical framework. Linking with the theories we mentioned in Chapter 2, there are mainly three parts of concerns about our research questions. By this knowledge, we structure the predetermined interview questions under the guidance of theoretical basis of trust, security, and threats. Starting with general questions, we are able to investigate the background information about respondents’ preference of mobile banking where we asked them about their general uses of mobile banking, the length of the period during which they used the service, and how much it added to their banking experience. After that we went deeper in the concerns of respondents about security issues, from there we started to direct them about
talking in the security by asking them about certain situations where they feel insecure as we aim from this question to get their insights about the surrounding environment and initiate the actual part of the interview, then we went to asking about network, application, security in the application and so on according to the following guide that we based on our chosen theories. In most of the cases we needed to ask more clarifying questions and follow ups to get more information.

Table 5 Interview design

<table>
<thead>
<tr>
<th>Question</th>
<th>Relation to theory</th>
</tr>
</thead>
<tbody>
<tr>
<td>How long have you been using mobile banking?</td>
<td>Background</td>
</tr>
<tr>
<td>How useful was it for you?</td>
<td>Background</td>
</tr>
<tr>
<td>How often you use mobile banking?</td>
<td>Background</td>
</tr>
<tr>
<td>What are the situations in which you feel less comfortable using mobile banking?</td>
<td>Situation Normality, user demographics (McKnight 2002, 2011) (Shin 2010)</td>
</tr>
<tr>
<td>Who is responsible in case of any security breach or loss of money happens to you?</td>
<td>Structural Assurance (McKnight 2002, 2011)</td>
</tr>
<tr>
<td>How is the application is working so far with you?</td>
<td>Reliability, Functionality, Helpfulness (McKnight 2011)</td>
</tr>
<tr>
<td>How much you know about security threats that are related to cybercrime and mobile banking?</td>
<td>Awareness of the known &amp; unknown (Komiak &amp; Benbasat 2004)</td>
</tr>
<tr>
<td>Describe the security options you observe when you use the mobile banking</td>
<td>Security mechanisms (Hutchinson &amp; Warren 2003) (Chellappa &amp; Pavlou 2003)</td>
</tr>
<tr>
<td>What do you think about the security levels provided by your bank’s application</td>
<td>Perceived security (Ally &amp; Toleman 2005)</td>
</tr>
<tr>
<td>To what extent would you perform monetary transactions in mobile banking?</td>
<td>Amount of transfer (Goeke &amp; Pousttschi 2010)</td>
</tr>
<tr>
<td>How do you think smartphones can differ in terms of security?</td>
<td>Type of device (Coursaris &amp; Hassanein 2002)</td>
</tr>
<tr>
<td>What are the specific situations or locations you avoid using the mobile banking?</td>
<td>Type of network (Coursaris &amp; Hassanein 2002)</td>
</tr>
<tr>
<td>What is the difference between your trust in mobile banking before and after using it?</td>
<td>Communicating security information (Linck et al 2006)</td>
</tr>
<tr>
<td>How the knowledge about mobile banking affected your trust in the service?</td>
<td>Usage experience (Shin et al 2010)</td>
</tr>
</tbody>
</table>

4.3 Sample selection
As we determined interview as our data collection method, we now continue discussing how to choose interviewees of our research. In some researches, the acquisition of useful data is performed through investigating the whole number of population. However, in this case, it is impossible to conduct a census. Since we will utilize interviews to collect data, it will take around 30 minutes for each interview. If taking a census, it will spend too much time on
collecting data. The other reason is, it is hard to reach everyone who has mobile banking using experiences and select valid data. Due to those limitations, we realize that our research objectives and research questions call for the high need of sampling.

Several sampling techniques can be utilized in business research, they can be classified into two main types: probability sampling or non-probability sampling (Saunders et al., 2009, p. 261). Probability sampling is more applied in those researches which obey survey and experiment research strategy. Every case in the population has equal probability to be selected as the source of research data in probability sampling (Saunders et al., 2009, p. 261). In other word, the samples are randomly chosen. Meanwhile, using non-probability sampling make it possible for researchers to select sample by their own criteria or some specific strategy. In our research, if we just choose samples randomly, it may involve someone who rarely use mobile banking or has little knowledge of that, which will not contribute to answer research questions, and may interfere with data analysis. Consequently, we agree to take non-probability sampling technique.

Thus, we start to select samples in guide of non-probability technique. With the goal of investigating users’ perception of mobile banking security and trust issues, we determine that our interviewees should have enough mobile banking using experiences. They need to have enough knowledge to answer our questions. Because now we are living in Umeå, Sweden, it is more accessible for us to interview people who are also living in this area. To screen out qualified interviewees, we try to category them by place they live (i.e. in rural area which is far from banks or urban are which provides convenient transportation to banks), age (young generation under the age 35 or elder generation). It has been proved that the high speed of younger people adopting new technology in their daily life like mobile phone (Katz, 2002, p. 293). Moreover, we also believe that the people living in the place where near to banks may influence the chance to use remoted operations of their bank accounts. To find frequent mobile banking user, we narrow the population down to people who living in Alidhem. First reason is, in this area, most of the residents are students from Umeå University, which indicate that they are young and may have the willing to try mobile techniques instead of traditional banking services. Besides, this area has only one automatically ATM machine, and its functions are very limited like withdrawing cash. It even cannot allow users to deposit money or check balance. Furthermore, the nearest bank is around 3.5 km far from here. Considering the occupancy of motor vehicles, we tend to hold the opinion that people who living in Alidhem do not have an economical and convenient access to banks. The samples of our research will derive from here.

For purpose of settling the research questions, it is of great importance to ensuring the data of our samples are valid when processing sampling procedure. Hence, we utilize availability sampling technique to confirm the respondents are active and willing to share their thinking and feelings to us. Through this, we believe all the data from the interview can be considered as relevant and significant. More specifically, we put up notices in public kitchens of several corridors, to introduce our research and recruit volunteers participating in the research. We list the important features we have mentioned above in the notice as follow: 1. Used mobile banking for more than 1 year. 2. Age is between 20-35. 3. Student in Umeå University.

As a result, there are 11 students contacting us, stating that they would like to participate in the interviews. These students compose the interviewees, in other words, the samples of our research are formed. Below we will give a brief example of the notice, and a form to give an overview of all interviewees.
Interviewees Wanted
Hi there!
We are two students from Umea University writing our thesis now. It’s about how young people perceive mobile banking and related security issues. So, we would like to ask you to share your mobile banking using experiences with us. If you are:
1. Used the mobile banking for more than one year
2. Age is between 20-35.
3. A student in Umeå University.
Please contact us!
Any private information collected is subject to the interviewees’ permission of sharing in this study.
Contact:
Amro: amr92agami@gmail.com
Tiantian: dutiantian818@gmail.com

Table 6 Details of all interviewees

<table>
<thead>
<tr>
<th>Number</th>
<th>Fictitious Name</th>
<th>Gender</th>
<th>Age</th>
<th>Date of Interview</th>
<th>Duration (minutes)</th>
<th>Background of interviewees</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interviewee A</td>
<td>Male</td>
<td>24</td>
<td>07/04/2017</td>
<td>22</td>
<td>International business development</td>
</tr>
<tr>
<td>2</td>
<td>Interviewee B</td>
<td>Female</td>
<td>22</td>
<td>07/04/2017</td>
<td>28</td>
<td>Finance</td>
</tr>
<tr>
<td>3</td>
<td>Interviewee C</td>
<td>Female</td>
<td>21</td>
<td>10/04/2017</td>
<td>27</td>
<td>Public health</td>
</tr>
<tr>
<td>4</td>
<td>Interviewee D</td>
<td>Female</td>
<td>24</td>
<td>11/04/2017</td>
<td>25</td>
<td>Chemistry</td>
</tr>
<tr>
<td>5</td>
<td>Interviewee E</td>
<td>Male</td>
<td>23</td>
<td>11/04/2017</td>
<td>21</td>
<td>Chemistry</td>
</tr>
<tr>
<td>6</td>
<td>Interviewee F</td>
<td>Female</td>
<td>26</td>
<td>13/04/2017</td>
<td>23</td>
<td>Marketing</td>
</tr>
<tr>
<td>7</td>
<td>Interviewee G</td>
<td>Male</td>
<td>26</td>
<td>14/04/2017</td>
<td>29</td>
<td>Marketing</td>
</tr>
<tr>
<td>8</td>
<td>Interviewee H</td>
<td>Male</td>
<td>22</td>
<td>14/04/2017</td>
<td>22</td>
<td>Finance</td>
</tr>
<tr>
<td>9</td>
<td>Interviewee I</td>
<td>Male</td>
<td>22</td>
<td>17/04/2017</td>
<td>24</td>
<td>Public health</td>
</tr>
<tr>
<td>10</td>
<td>Interviewee J</td>
<td>Female</td>
<td>25</td>
<td>17/04/2017</td>
<td>25</td>
<td>Physics</td>
</tr>
<tr>
<td>11</td>
<td>Interviewee K</td>
<td>Male</td>
<td>26</td>
<td>18/04/2017</td>
<td>23</td>
<td>Robotics and control</td>
</tr>
</tbody>
</table>

4.4 Interviewing process
We come up with two methods to conduct the interviews. At the beginning, we prepared to work together. Which means, in the interview one of us will talk to the interviewee and ask relevant questions, the other is responsible for recording and taking notes. However, due to the time limitation we finally decide to split the tasks evenly between us. That allows each of us can participate in interviews and having chance to talk to interviewees. A traditional interview method, face-to-face interview, is adopted in order to get a comprehensive understanding of interviewees’ feeling. Face-to-face interviews make it possible for us to adjust the context of the interview through different features of each interview. To reduce distractions and ensure the accuracy of data, we emphasize a quiet communicating environment. All the interviews are held in group study rooms in university library. We also record all the interviews for the sake of losing any important information. Because in most cases people would like to talk more and share their ideas in a comfortable and friendly
environment, we prepare coffee and snacks before the interview, and give them a small talk about ourselves. We stay serious and professional during the interview. Although the duration of interviews varies from how talkative the participant is, we encourage all of them talk as much as possible. As a result, each interview last around 20 to 30 minutes.

4.5 Transcribing and analysing the data.
After recording the interviews, we had to transcribe and transfer the data from audio form to written form, which has generated masses of data, we removed the parts we did not see as necessary to reduce the amount of data generated we transcribed the whole interviews and took some quick notes as well to help us in the ones to follow. According to Saunders et al. (2009, p. 485) the researchers should not only be interested of what the participants said but the way they said it. We focused during the interviews also on the non-verbal cues left by the participants and recorded them in order to use them later in the analysis. Transcribing the data was a time-consuming process, and each interview took approximately 4 hours to be fully transcribed. Later after data transcription offered the interviewees a list of the quotes that we are going to possibly use for them to check their mistakes and confirm with them what they have said during the interviews.

After transcribing the data, we needed to prepare it for analysis. In analysing the data there are two approaches used that are induction and deduction. Because we chose at the beginning to use an inductive approach as it suits our qualitative nature of the study we analysed the data in accordance with this approach that is we had to start collecting the data and explore them to see relevant themes and issues to follow up and concentrate on (Saunders et al 2009, p.490). In analysing the data there are three common types of qualitative analysis processes which are: summarizing the data, categorizing the data and structuring of data using narrative. Summarizing the data involves writing up notes or producing a transcript that summarizes the interview into brief key points, while categorizing the data refers to developing categories and attaching those categories to meaningful chunks of data (Saunders et al 2009, p. 492). We used in our analytical process the categories in a way that is we developed categories from the data in order to identify and recognize relationships and themes we need to use in our research and draw conclusions.
Chapter 5: Findings

In this chapter, we present our qualitative data in the light of our respondents’ responses. We identified relevant themes and we categorized them. The findings are presented according to the themes identified of our collected information.

5.1 General Attitudes and perceptions

For most of our interviewees their attitudes about the mobile banking service is trustful rather than worrying, we examined the degree to which they are satisfied by their services and the majority pointed out at that they are comfortable using the service with relatively low level of concerns. Such concerns exist of course but are low. Suspiciousness was not notable except for one or two participants, the ones who had previous negative experiences within the m-commerce context.

The users are more open to other innovations around mobile banking, they expect good growth in the use of the technology, most of them indicated that they will continue to use mobile banking despite the concerns they have. The level of activity on average for our participants was between once and three times a week so we cannot say that they are active users especially, the international students who have no access to the Swedish banking system so they do not use other services associated with mobile banking such as mobile payments or mobile commerce. Generally, we divided the relevant themes we found into 3 main categories according to our chosen theoretical concepts, and what we have found most relevant for our thesis topic.

We asked our interviewees how they perceive the security in mobile banking when they use it in their normal situations and for doing the transactions they do normally. The general replies we got that they perceive the mobile banking is fairly secure and had positive confident opinions, however only one interviewee felt otherwise and that the security of mobile banking needs to be improved. We added another question to compare between their perceptions of security of banking from a mobile phone with banking from computer. Five of the respondents replied that they feel the computer banking is safer while the rest saw no difference. The reasons we found to make computer banking more secure than mobile banking was that the computer banking was more familiar and easier to use and according to the interviewees it just feels safer for them to do it on the computer as it has bigger screen and keyboards so they believe that the margin of error is less than doing it on mobile phones.

In the following subchapters, we explore our results about security perceptions and the awareness of the different visible security mechanisms to the user, then followed by the threats perceived by our interviewees and their levels of awareness.

5.2 Trust in mobile banking

When we discussed trust in mobile banking, users trust levels of mobile banking, they referred to mainly three categories we identified and will list in the following sections. We also found that their levels of trust differ from context to context, the application of mobile banking used and the assurances from the banks about security damages and compensation. We found that some users of mobile banking can have different levels of trust in the mobile banking: the surrounding environment or place, the bank itself and the application of mobile banking.

5.2.1: Institution based trust

A relevant theme our interviewees talked about is the assurances of the banks, most of users indicated that they are not worrying about the mobile banking security issues that might happen to them simply because they see that it is the responsibility of the banks to provide the
protection required for their users, and that they can have to support of the bank in case of any
security breaches so for them, unless if they gave their information too easily and then it is
their responsibility. There is a clear reliance on the banks to compensate the damages that
result from the users using the mobile banking application where most of users said that they
can get refunded in case of missing money or anything happens to their accounts.

“If there is a suspicious money withdrawal from my account with proper investigation, I can
deny any transaction I did not process and the bank will return me the money” Interviewee A.

“My card has been copied from someone in the US and tried to steal money from it, but my
bank immediately discovered the transaction, locked the card and called me to arrange a
shipment for a new one, I think they did a really good job and it is their responsibility to keep
their clients’ money secured” Interviewee B.

The assurances were part also of convincing those users to adopt the mobile banking
application for the first time, where four of our interviewees said that they were suspicious
and do not trust the new technology to use it for the first time but the bank worked on
convincing them and assuring them of covering possible threats and monetary loss of their
mobile banking account. They said the bank provided them with all the necessary information
about the technology and how to use it in the best and safest way addressing any possible
limitations of the technology.

“My bank told me for the first time about the application and convinced me to use it. They
provided guarantees that the application is being protected and totally safe to use and it will
help me a lot with my banking” Interviewee C.

Despite the assurance of the bank on compensating the users for their monetary loss, two
respondents experienced doubts about their privacy and their information loss, stating that
they do not feel comfortable when the bank is using their information for purposes they do not
know and that they know about bank practises when comes to use their private information
and that even banks infrastructures are vulnerable to be broken down and attacked by hackers
despite the guarantees and policies stating the professionality of the bank to use their
information. While other respondents declared that their trust standing in the banks to
protect their information and that they have the necessary equipment to maintain and protect their
information

The other theme we found according to our interviewees Is the situation in which they use the
technology, the trust level and security perceptions in mobile banking has changed when they
switched countries or continents where the difference was not only the bank but demographics
and culture which has affected the trust level of interviewees whether positively or negatively.
The influences were mainly found to be: in social circles, communities, relevant media and
news, distance and communication. One of our interviewees mentioned that she does not trust
the mobile banking in Sweden because she thinks that the system is too easy and that she does
not feel secure about it, while another one from Egypt had similar opinion talking about the
social effect on mobile banking trust, where he said that the culture and society there in the
country prefer to handle monetary transaction face-to-face and that they trust paper money
rather than cyber money, he continued with the effect of that on him as it formed a negative
picture of the mobile banking as people are not using it.

Two of our interviewees talked about their preference to bank in specific countries like in
Sweden because of that systems and reputation of banks are secure in addition to minor
security issues have been heard about security accidents related to mobile banking and banks
in generals. The context of the place which our users find themselves influence their trust in
the bank and banking behaviour like the general acceptability of the technology, the social circle opinions and history of specific incidents that shaped their opinions.

“*In Sweden, people trust each other so it would give you the feeling of safety and security being in the country and there would be no worries of someone stealing your money while in other places I would be more cautious when I use my mobile banking*” Interviewee D.

“*In my home country, most people use paper money and they do not use mobile banking although it exists but they still do not trust the electronic money and prefer to carry cash with them most of the time*” Interviewee E.

What we noted that what alters their perceptions in certain context is related to the society and culture in that context as it plays a role in their general perception about the technology of mobile banking. The surrounding society can either help and encourage on adopting and trusting more the technology like our interviewees who lived in Sweden and experienced living abroad they said that the people factor is playing a role in forming being more or less suspicious about the technology, also our Egyptian respondent pointed out that when he generally listens and discusses the mobile banking technology either with the bank their or around his friends or circle where people there are generally more suspicious about the technology and the general feeling there does not promote to adopt the technology there. Similar to other interviewee who said that in Russia the society there is more risk about everything and the rates of crimes and the likes are higher than in Sweden so for him it plays a role. For the rest of our interviewees most of them were in Europe and they did not experience any change in their level of trust or security beside the applications themselves or the technology itself.

5.2.2: Users’ propensity to trust

During the part of the interview when our participants talked about the level to which they rely on the mobile banking in their banking transactions in daily life. Four users claimed that they use the mobile device for different type of banking transactions and mobile payments and that they rely on the mobile device heavily for their banking purposes. They stated that since they used the technology they saw a big difference in their banking activities and that it saved them a lot of time and effort resulted from using it across many situations and places, which has led them to form positive expectations toward this technology and that they are likely to adopt it in other countries and situations where they need to change the bank they are dealing with.

“I have used a lot the mobile banking and It had improved a lot my banking experience. I expect to use it more in the future.” Interviewee F.

“Using the application has contributed a lot to the way I bank, and I like each time I take the mobile phone and connect to the application even to check my balance. I always feel in control when I constantly check my account balance on the move” Interviewee G.

Other five respondents said that they have average dependency on the mobile banking service, stating that they use it few times a month when they pay the basic monthly bills like rent and money transfer, while for their daily payment they use credit cards and cash. They showed that they still prefer those ways of payments instead of doing everything on the mobile application because they do not trust yet the digital money and that they have some security concerns over using the mobile all the time for performing transactions.

“I use the mobile application few times a month just to pay rent, I do not trust the technology entirely yet, and I still prefer the use of cash and credit card, it is safer.” Interviewee H.
“I do not use mobile payments because it is not available everywhere I go, so it bothers me to switch from one payment method to another, so I use electronic and mobile banking to do big things” Interviewee C.

The rest of the respondents shown low involvement in mobile banking where they stated that they use the application rarely and that they are still not comfortable with it. They still have preference for internet banking over mobile banking because it is easier and simpler, therefore their usage of the service was not high as they have higher functional replacement and preferences.

“I do not rely on the mobile banking much, I still prefer other ways of paying and transferring money especially the old ways and cash payment, I am not a fan of technology and I am more like the old people, so unless it is very effort and time consuming to do it in person I will not use it.” Interviewee B.

5.2.3 Trust in technology

For the application of mobile banking, many customers talked about the mobile banking application they have, and generally they all have different kinds of mobile banking applications with different characteristics, strengths and weaknesses, we list main sub-themes under this category according to what our interviewees said about the application in terms of reliability, functionality and helpfulness. When asked about the technology level of functioning and operative attributes our respondents shown different opinions in terms of the three dimensions of trust in the technology.

For reliability of the mobile banking technology in general all customers agreed that they want the service working properly and in uninterrupted way, where they spoke about their need to have an application that works all the time everywhere they go, especially that our interviewees are from international background and like to travel so they believe that banks should be able to expand their capabilities abroad and offer them their services also abroad in addition to keep the application up with performing regular updates and fixing errors and bugs that might arise. Four respondents talked about what they think in terms of security when they observe the technology reliability.

The respondents said that having an application that is reliable and practical can make them less worried about being secured. Two Respondents said that they sometimes experienced several errors and connections problems which has caused them to feel worried about losing their data where they had to re-enter their banking information again when using the mobile banking service. Another respondent said that the application each time updates itself to fix bugs, or improving performance this has given both good and bad impressions to the user where he stated that he appreciated that the bank is constantly updating the service, while on the other hand it indicates that there are security issues within the application that the bank is working on. The last interviewee said that he experienced using more than one banking application from different banks and the speed of performing a transaction differed between both application, that indicated for him that the application is slow and that it takes extra seconds for the app to register the transaction which leaves the screen open with the banking information and therefore he may want to hide the screen until the transaction is registered.

“I have seen some interruptions and experienced lags when I do a transaction on mobile banking because of the connections, it annoys me if I have to do all the process again” Interviewee H.
"I receive new upgrades for the application each once and a while, it is good that the bank is working to improve it, but it may mean also that there are security problems they are solving and that their system is not secure enough" Interviewee J.

"In another mobile application I used, I noticed that it takes the new app more time to finish the transaction. When I press confirm the screen freezes for few seconds and then the transaction is done. It has not happened with my old application” Interviewee I.

About the functionality the application that delivers, our respondents talked about the various attributes that the mobile banking service delivers to them, we selected the ones who are related to security as part of the mobile banking service functionality and how the security features are perceived according to the participants who gave us answers about them. Two participants have talked about the security features provided by their mobile banking service from their bank and praised those features as part of the functionality of the technology where they stated that the they appreciate the security features their mobile banking promotes. Where one user said that the mobile banking has several security warning steps when performing a transaction, while another respondent said that after ten seconds of inactivity the application logs off.

“I think my bank has a strong security system, in each step I find a message within the app states that the data are safely secured and store within the bank’s database” Interviewee F.

“If I did not log out after ten seconds, the application terminates by itself, this is good because If I forgot to log out someone may use the account.” Interviewee I.

5.4 Application Quality

For the application of mobile banking, many customers talked about the mobile banking application they have, and generally they all have different kinds of mobile banking applications with different characteristics, strengths and weaknesses, we list main sub-themes under this category according to what our interviewees said about the application in terms of Application design, information collection, application reliability, communication and innovation.

Application design was for most users a strong indicator for the intention to use the mobile banking application, and understanding the application basic functions, combining functionality with simplicity to make transactions faster, easier and simple. Five of Our interviewees believe that the visual characteristic can be strong factor improving perceived security and feeling of trust especially the clearness and the accuracy of information as they stated that if the information were not accurate that leads them to lowering they perceptions while other two respondents talked about the simplicity of the application and that they want no complexities around using it as they want it to be quick and simple.

When asked about the design features they prefer the most, we had mixed reviews from our interviewees depending on their background as one user says that for her the language of the application plays a role in her trust in the application, as she talks about the Swedish application she uses that has no language option and that she cannot use it or perform transaction without understanding what she is doing, while another talked about the innovation and the different features the application has and stressed that he would like to have several features that within which he can use, not only checking balance or performing transactions, but things like chat options or location services. The colours of the application were also mentioned by three interviewees who said that their mobile banking applications have nice colours and that they used several mobile banking applications before and each had different colours that resembles the brand of the banks they are using.
“I cannot use banking application that I don’t understand, it bothers me and makes me leave the whole thing if I do not know how to use it” Interviewee D.

“I will not trust a poor designed application even if it has the strongest security, I would want an application that projects good design and I think that can tell more about security than the security features themselves” Interviewee E.

One user said the design for him is so important in using the mobile banking application, as he had experience with a poor design application that has led him to quit the service after a while because he preferred using the computer instead as the design of the application was poor and worse than the one on the website.

We asked also our interviewees also talked about the performance of the application, around four of the respondents said that the performance of the application is important indicator for their trust in the application, the speed in delivering transactions especially abroad and how accurate bank can perform the transactions on mobile banking. Regular updates for the application is appreciated as they get the sense of that the bank is coping up with the service and performing the necessary upgrades and improvements for the platform, one user said that he thinks that updating the application can mean a security issue as he noted once in the application description that was available on the application store on his device.

“It was written that the new version contains upgrades in the security and performance, I think it shows that they are working on their mistakes but at the same time it means that there are actual security issues to fix” Interviewee F.

For him it meant that there were some security gaps and he perceived this step as both worrying and welcoming as he thought that it might mean for him that there are security and performance lag that need to be update, and he was content that the bank is working on improving it. Bad performance of the applications meant that the application is not invested in properly and the bank did not do enough to create a good platform which can cause users to switch back according to some responses we had from our respondents.

On communication, we asked our interviewees about their opinions about the communication process with the bank when it comes to communication of sensitive information. Few of our respondents preferred to communicate with their bank on the application stressing on that for them they would wish if they could for example reset the password or other credentials on the application by having a secure chat option where they can exchange information safely, as they think that going to the bank in person is a long process and time consuming, while the rest preferred the personal option where they go in person to the bank and receive or modify the information directly with the help of the employees. They think that it is more secure than any other way. We asked also about what kind of security messages they receive from the banks concerning the mobile banking application, seven respondents claimed that they receive warning messages from their banks when they are using the mobile banking service from an unsecured or public network, notifying them about that the connection is risky, another kind of messages is e-mails from banks about their denial of every kind of messages that ask them to provide personal information about the users where the banks assured that they do not request any kind of information by the mail from users as some hackers try to copy bank mail formats or other formats to trick users into giving them personal information, another form of warning communication is mobile phone calls where the bank calls the user to inform about any security breach as one respondent explained when he suddenly found that the bank locked his credit card because they was a suspicious activity overseas received two days later a phone call from the bank about this incident. Two other respondents said that they have no
messaging feature on their applications adding that they prefer to have this feature instead of communicating over the phone, e-mails or computer banking.

“My bank sends throughout the year several questionnaires to asses my opinion in regard to their mobile banking platform and other services” Interviewee D

“I receive messages from within the application warns me that the connection is public and insecure and It logs out automatically whenever being used in publicly opened networks” Interviewee B

“When I reset my password of my online or mobile account I go to the bank in person because I do not trust being sent to me by any means. This way I can make sure that only me who has the access to the letter” Interviewee G

5.5 Visible security mechanisms
The general security knowledge of the study participants was important aspect in our study so, it was included in our interview questions. We asked about participant’ awareness of the security features or mechanisms that they deal with when using the mobile banking, we noticed that our respondents consider themselves generally uneducated about the technical aspects of security features. The level of knowledge about security mechanisms though varied and we found differences according the background of the users who participated where we found for example IT students we interviewed more knowledgeable about it in comparison with others.

The interviews included the visibility of security mechanisms to mobile banking users. Our responses indicate that the visibility of security mechanisms vary according to each user. The most mentioned features of security were the mechanisms of authorization, authentication and privacy which is represented in digital identification, user credentials and fingerprints and security confirmation codes in addition to privacy statements that are seen when using the application. These the mechanisms that are required to sign in the application of mobile banking and authorize transactions. About the visibility of the authorization mechanisms. All the users reported that they use mostly user names and passwords to log in their applications such method is presented by most of the banks they are using, however two interviewees who live in Sweden pointed out that they are using digital ID as part of their personal identifications and when we asked them about how they feel about such security steps, the first one responded that he appreciates the existence of a digital ID as it gives him more security to the mobile banking application and in this case he can only log from his phone, while the other participant agreed also on being a good measure to implement the digital ID however he mentioned that it may not be so efficient because it restricts the use of the mobile banking to only one device which if lost or stolen can represent a problem.

“The application of Mobile Bank ID in Sweden is a very good improvement; this service allows you to secure more your mobile banking and also use it for governmental service.” Interviewee K.

“The Bank ID is very useful and secure however if someone stole my device or I lost it, then I lose access to my bank, my bank provides me with other methods to log in without the Bank ID but not on the phone, it is over the internet. On the mobile phone, I have to install on it the bank ID application first to use it which can take time” Interviewee B.

Another interviewee said she uses fingerprints to access his mobile banking account, which is similar to the digital ID, however according to her she thinks that the fingerprint option is more personalized and more difficult to replicate.
“If a hacker wants to hack me he has to get close to me in person a copy my fingerprint which I think limits the options for a hacker to get in the account, I think the fingerprint is a good option because its more personalized” Interviewee D.

Another interviewee who had experienced using the mobile banking from different banks in different countries, compared between the banking in Sweden which applies the use of the digital ID and his bank in Ireland which uses a combination of three credentials used to log in the application using username, password and date of birth. He thinks that the latter is more secure the first.

“The digital ID is good in Sweden but it still Sweden and generally speaking it is here safer, but technically speaking I think my home country’s bank uses trickier method to log in the application, three digits of my code, plus the date of birth and the username, while I would need only a code plus the digital ID installed on my device” Interviewee E.

We also asked about the authentication mechanisms and their opinions about it. The authentication mechanisms we observed that was mentioned by the interviewees included mainly the use of fingerprints and a special authentication device that authorize the transactions after logging in the application. The respondents who talked about having such mechanism were three while two other users did not have such tools and for the rest of the respondents we could not get such information because of the time of the interview. In using authentication mechanism two respondents said that they are using a device that generates a code and that personal device is given to the user upon activating the internet and mobile service.

“I use a special device that generates codes whenever I need to perform a transaction whether on mobile or on computer and internet banking, it think it is good because it adds to the security level I have, the problem though that it is not efficient because I have to hold the device with me and not lose it” Interviewee G.

The other user uses her fingerprint to authenticate the transaction instead, she stated that she uses her fingerprints both times when she logs in the application and when she authenticates a transaction, for her there are no worries about losing the device because she uses her fingerprints instead.

“I use my fingerprint to access the account and to authorize any transaction I do on mobile banking, it was better than before when I used the special device. Now I log in and do everything on one device without needing another” Interviewee A.

We asked also our respondents about the security steps when authorizing a payment or a transaction using the mobile banking and how do they feel about it. Two respondents claimed that they only need to sign into the application to be able to perform transaction stating that once they log in they are able to any transaction without extra steps to be done, while the rest of the respondents have different additional steps that add to the security of mobile banking application where some had an authentication device they keep with them all the time, and with that device they can generate codes and enter it before doing transactions, while the others had to enter the password each time they perform a “new” transaction for a new destination. Respondents in general preferred having this extra step when performing transactions on mobile banking as they had worries that someone will be able to crack their accounts and manipulate their information so they were in favour of adding extra authentication or verification step when performing a transaction, while on the other hand only one respondent claimed that he prefers the speed rather than complexity of security adding that he does not want a complex secure application and that simple security is enough
as he wants the mobile banking application to work quickly and efficiently he even stated that he prefers to save the password on the device in order to avoid entering the login credentials each time he uses the service.

“In my application, it takes only to log in and then you can do whatever you want with the application, the logging-in process is good in terms of security but it is just one step and I think it is not enough” Interviewee B.

Regarding the application privacy and collection of information some customers did not care that much about having their information collected by the banks using the application, others were more reserved stressing on that banks need to disclose about everything they would collect from their customers and what do they do to collect the information and how they protect the information. The believe that banks should collect information about users in accordance with the law and regulations as they perceive their privacy is something sensitive for them, and that banks should involve a privacy policy about what type of information they are collecting. Five respondents claimed that they want to know how banks are collecting information from them and for what purpose where they stated that they also see a window on the application that explains them the bank’s privacy policy and the process of collecting the information on the application, while the others stated that they do not look for any privacy disclosure agreements or windows on their applications.

“I don’t mind my information being collected from the banks, but I would want to know why and what are they going to do with it.” Interviewee K

“On the application, there is a tab or window that when I click on, it displays the banks privacy policy regarding the use of mobile banking application and privacy settings, I think it is good that they displayed it in the app” Interviewee D.

5.6 User experience
We asked the respondents about their past usage experience in mobile banking and how their levels of trust and security perceptions differed from the moment they started to use the service. Most of the respondents were suspicious at the beginning when they used the service as they were not familiar with the technology and said that the banks advised them to use the mobile banking application as it will make their banking experience easier and simpler. Their experience toward the mobile banking affect their levels of trust and security perception both positively and negatively.

two of our respondents experienced negative mobile banking experiences. The first one had money stolen from her account after buying goods online, her mobile banking account was linked to the online payment company as she makes purchases online from the mobile phone. When she moved to Sweden she found 250 euros missing and reported the bank which investigated the incident and returned the money. The respondent after that cancelled her account with PayPal and she now feels less secure about using this feature in mobile banking and said that she only uses it to pay the rent. Her experience with the mobile banking has affected her security perception of the service and caused her to be more careful when using it.

“I lost money when I bought from PayPal, it was linked to my mobile banking account and suddenly a message from the bank told me that money is missing after authorizing them, I contacted them after but they did not reply to me, I do not trust them anymore” Interviewee H.

Clearly this experience has impacted her online behaviour of mobile banking where she assured that after this incident she stopped using the application except for necessary things and will use it again after going back to China. Another negative experience was for another
respondent who had not been affected by security but by design and poor application features leading him to quit the mobile banking service and return to the computer banking. As he did not know how to use the application and that it was not functioning properly which caused him to prefer the use back the computer.

“I had with my home country, my bank a bad application with poor design and a lot of errors and I could not use it, for me it was not simple and I used since then the internet banking until now” Interviewee J.

For this user security of the mobile banking application was not related to his perception of mobile banking because he was talking about his experience with the application design and functionality.

Other respondent had passed through a positive security experience that fortified his trust and security perceptions of mobile banking and his bank in general, the experience was not related to mobile banking but the outcomes from that experience can be reflected on the mobile banking as well, where he got his credit card copied by the ATM machine by using some trick from people who later used the copied numbers and attempted to make a purchase later.

“The bank locked my online account and the card I am using temporarily then contacted me to investigate this issue, they said they were suspicious because they spotted several different activities on different locations” Interviewee G.

5.7 Amount of transfer

We asked about our respondents’ opinions on their usage of mobile banking and levels of trust and security perceptions in regard to the amount of monetary involvement whether in transferring money on mobile banking or in keeping their savings in an account that is connected to the service. For the first matter, our respondents shown variety of opinions in this regard where five respondents claimed that they have no security worries over the amount of payment or transfer they perform on the application. They stated that the mobile banking for them is similar to the transaction on computer banking and that there are no certain limits of amount of money transferred via the mobile banking channel that would make them change the channel, on the other hand there were opinions that were on the contrary- subject to safety preference in regard to the amount of money transferred, one participant mentions for example that he do not feel entirely safe when transferring amount of money that is large and that he prefers to do it from the computer.

“I do not mind transferring big amounts of money from the mobile phone, for me the mobile device and the computer both use internet and I see no difference, it is just waste of time if I switch” Interviewee I.

“I prefer using the mobile banking for small amounts of payments, this way is less risky and faster, because if I think about making bigger transactions it makes wander and think a lot about taking longer time to decide” Interviewee K.

The other matter in regard to the monetary amount is the amount kept in the mobile banking account, since our participants are younger and from college background, they do not possess large sums of money so they talked about it hypothetically. Only two of the participants have shown doubts over putting large sums of money in account related to mobile and online banking, they attribute that to certain factors such as their overall risk aversion, their tendency to not to save the money in liquid form and splitting their savings over several different accounts.
“All my accounts that I have, have the online and mobile service, for me If I would split my money over these accounts because if something happens to one of them, I would split the loss this way, kind of not putting all your balls in one basket” Interviewee J

“I would only install the mobile banking account when I intend to use it in the future, right now I use the internet banking, it would be perfect for me if I split both accounts so one is for mobile and the other is for online banking, this way I would control how much I put on the mobile banking one” Interviewee H.

While for the rest of the users they have no notable opinion on the matter, they indicated that they have no problems in regard to this matter.

5.8 Device

On the device related perceptions, we discussed it with our interviewees during the interviews where we found that the related themes or reasons that would affect the perceptions of security of the device for mobile banking users are either the fear of losing the device, altering the device software (Jailbreaking) and installing unknown application. Eight of our interviewees shown worries about losing the device where five of them stated that they have personal and private data that they do not want to lose, one of them said that he keeps some important notes on the device such as usernames passwords for some of his e-mail addresses and also the PIN code for his credit cards as he uses more than three different ones, while the other three stated that they are dependants on the mobile banking and losing the device would put them in a trouble where they find themselves without access to their finances.

“I keep my mobile device with me all the time, and I have some private pictures and information that I do not want anybody else to see, I am not worried about losing them, because I have a backup for them, but just the fact that they might fall in the hand of others that worries me” Interviewee D.

“I keep important information about my e-mail addresses and passwords, also PIN codes for my credit cards because I cannot remember them all and I use many of them so I keep them on the device, and if I lose it, it is going to be a big problem for me” Interviewee F.

“I use the mobile for everything related to my bank, payments, money transfer and account balance and I travel so often so If I lose my mobile phone I would lose access to my account” Interviewee E.

We asked our about what difference they see in security between the mobile devices and software they have. Two responded with the fact that for them they know about difference in security levels between each device software where they state that apple devices are generally more secure because the applications available there are more monitored by the company and that they have a policy that does not allow for open developing programs and applications unlike Android devices where the application there that are available on the google play store are more open system and it allows various developers to create and develop applications which makes the system more vulnerable as it allows more freedom to develop infected application. One respondent talked about changing or rooting the device software and altering it in order to bypass the security of the application store in what it called Jailbreaking which refers to modifying the software of Apple devices to allow it to bypass the application store and install many other tools and application that were not available before, these variety of tools is tempting for users; however, the probability of hacking risks are higher. The rest of the respondents did not see any difference between the mobile devices in terms of security.
“I jailbroken my iPhone 5, two years ago, I wanted to have more access to applications, I know it’s riskier but I think there are many more things available on Cydia rather than the normal app store” Interviewee G.

“I did not root my android device but I know that rooting the device would increase the chance of insecurity of the device” Interviewee K

Rooting or altering the device software allows the user to install and have access to applications developed by third party, such applications are not monitored by the software of the original company of the mobile phone, in general about the applications we have one user who mentioned that the applications installed on his device normally require access to the device information, he has doubts thought about the fact that applications ask for permission to access data, he does not know exactly what the application are getting in terms of information.

“I do not know what information they are getting, but they ask for my permission and I give it because I need to use the application, otherwise without the permission I cannot use it” Interviewee F.

5.9 Network and connectivity

When we talked during the interviews about how network and connectivity may concern the participants in terms of security when using the mobile banking. The participants responded by mainly mentioning two related things that might concern them. The first one is the stability of the connection of the network, while the second one was the type of connection they are using to connect the mobile banking service with. For the stability of the connection, one participant indicated that she feel less secure when they are subject to interrupted signal or connection where she are experiencing that during using the mobile banking they feel afraid of entering and losing the personal data associated with the transactions, she indicated that she lost the signal when using the mobile banking application as she used it to perform a transaction and after entering her data the page was gone and she felt less secure after that fearing that the data she entered went somewhere else.

“I felt for a moment scared as I was waiting to reconnect again to the internet and use the application again, I don’t know if the transaction is process or what exactly happened” Interviewee C.

The other thing associated with the security perceptions when it comes to internet and connections was the type of connection or network users are using. Three participants indicated that they feel different level of security when they are connected to public Wi-Fi, cellular data connection and home. Such feelings come from the strength of the security of the network and the existence of other people who are connected to this network.

“I prefer to use mobile banking only from my cellular data, I think the difference is that when one is connected from cellular data its safer because its directly from the SIM card” Interviewee E.

“I think any type of Wi-Fi is less secure than the cellular data, because some people who connect may get you IP address and through it they can hack or whatever they do. It is just the ability to see other people who are connected on the network, while this thing is not available through cellular data I think” Interviewee J.

“I always avoid connecting to an open Wi-Fi networks especially the ones with no passwords, since they are open I think you do not know who is also connected and what they can do” Interviewee A.
5.10 Other concerns
Apart from losing the device itself, or the network and connection. 6 interviewees had some concerns regarding spam e-mails they receive on their e-mail addresses. These emails contained suspicious links and ask them to provide personal information they do not want to share, things like lottery or any other fancy title that tempt the user to give any kind of information about themselves such as their mobile phone numbers, home addresses or other things. Another concern was suspicious links they receive from social media sites such as Facebook or LinkedIn.

“I receive often e-mails with fancy titles, such as earn a lot of money from your home, or you have won the lottery, or other things that may contain links to open.” Interviewee F.

5.11 Familiarity
When asked about our respondents’ feelings and perceptions of the mobile banking service before and after adopting the service, seven people responded that they were suspicious and worried about the new technology because they were not familiar with and they did not know how to use the service, nor how security mechanisms work or various application features, so they were sceptical about it. They stated that they wanted to adopt it thought because they were excited at the same time to observe other people using it, and the value it might add to their banking experience and now after using and adopting the technology they are more comfortable with it and that they know now the technology and it became essential part of their lives. Three people said that their family members encouraged them to adopt the mobile banking technology, while other four respondents said that their banks talked them into adopting the technology convincing them with its benefits and effort & time reduction to the users. While one respondent stated that in his country people perceive the technology of mobile banking as un trustful and unsecure because they trust primarily the paper money and not mobile payments.

“I did not trust mobile banking at first, but later after some time I got used to it and it is very useful” Interviewee I.

“My bank first convinced me to download the application because they said it is so convenient” Interviewee C.

“In my home country, nobody talks about mobile banking and when they do all what they say is that they are afraid of transferring their money using it” Interviewee E.

5.12 Level of awareness
Because users level of knowledge about internet threats is vital to their security as it contributes or prevents security threats, we attempted to discuss this in more depth with the customers. Our discussion covered the existing knowledge of the participants in several areas including their levels of knowledge about various threats that surround the mobile banking, the sources they get their information from and the mistakes they believe that might affect their mobile banking security experience.

For the level of awareness about security threats we divided participants responses to two categories, one group of users were more knowledgeable about different viruses and mobile infections that might attack the device, while the other group was did not have the technical knowledge but they know about accidents and hacking losses that they know about, the responses from the firs group were as following: one person indicated that he knows what is malware and what it does to the mobile phones in terms of threats and losses to personal information, that user applies various mobile antivirus and antimalware application on his device because he is aware of such infections.
“I installed antivirus on my mobile device, I think most of other users should do that as well because the viruses are attacking mobiles as well as computers” Interviewee F.

“I know that hackers from obtaining your IP address can gain access or get information about the user, and I read about some internet providers sell such information about users” Interviewee K.

The other participants did not show technical knowledge about threats that affect the mobile devices, but they have concerns and they heard about what losses can happen from attacking and hacking the mobile device and internet banking accounts. One participant for example stated that he knows a person who had his mobile phone locked with a message from the hacker asking for a ransom in order to unlock it again.

“The hacker threatened of deleting the data if he does not pay 10 euros, He could not do anything with mobile phone except going to the link they posted on the message, it is like apple’s feature of tracking and locking your lost phone except that it is not apple who did this.” Interviewee D.

Another user stated that he read in the news about an identity theft that happened to a mobile banking user through copying the phone number then managing to know some personal information about the user from the telecom company and attempted to ask for a sim card replacement to later install another mobile banking application of the victim account.

“I read about it when I was browsing the internet about how safe is the mobile banking application during the first few weeks of using the application” Interviewee I.

5.13 Users suggestions to improve security

We asked our respondents to give suggestions about the future of security in mobile banking application that will improve the security of the service, overall the respondents did not have long comments on the questions and six of them were already satisfied with the level of security. The comments we got about it is about improving the logging in method, where they expressed the need to have alternative options to log in the application such as drawing pattern like the one used to unlock an android phone, or having a feature that enables facial recognition through the front cam, or fingerprints. They suggested to have these options as alternative way in case they forgot the credentials so that it saves them time and effort to contact the bank to reset everything. Another suggestion was for those who have already one authentication step to perform transaction was to add another authentication step where they confirm before transferring the money by entering a code or just confirming in anyway as they were having some concerns about the possibility of getting hacked and losing access to the account, while the hacker can modify and do anything with the victim’s account, in addition to install an anti-malware on the device to protect it from viruses and Trojan horses.

Another opinion by one interviewee who expressed his preference to speed and efficiency rather than complexity of the service security where he stressed on having less levels of security in favour of the application speed. His logic was that the mobile banking is a light and easy to use service and should not be complex and difficult to the users, and that complex security will lead to user frustration and less application-use.

“It is good to have more than one way to log in the application in this case you don’t worry about losing passwords” Interviewee G.
Chapter 6: Analysis and discussion

_In this chapter, we analyse and discuss the empirical findings in the light of the literature covered. We will demonstrate in how far our results compare with our theoretical background of this study. We present the analysis part with same titles and themes which we drawn from the literature starting from trust concepts and theories going, further into security perceptions._

6.1 Users Trust in Mobile banking

6.1.1 Institution-based trust

Our findings about this aspect indicate that user’ beliefs about trust in the mobile banking were affected somehow by the situation or place they found themselves in, such as being in a foreign country with different banking systems, different people attitude and different social circles that affected their trust and security perceptions. According to the results we found that this change was mostly with students who were coming from different continents with different backgrounds and it happened only with people who came from different continents.

Our findings about the social context of mobile banking corresponds with (McKnight 2012 p.12:2) definition of situational normality, which is the belief that success with a specific technology is likely because one feels comfortable when one uses the technology in a normal way in a specific setting, our respondents were not comfortable with the technology of mobile banking when they switched countries. This corresponds also with (Gefan et al., 2007 p.7) the social presence in which the medium is being used which is the social environment in which the mobile banking application and sensitive information are being exchanged, our finding also corresponds to (Shin 2010) user demographics stating that user demographic, location and culture of the user can affect the security perceptions of the user.

Our study covered also the side of structural and bank assurances that ensure the user protection against security and service errors. Our study revealed that the perceptions of security are strongly impacted by the structural assurances provided by the banks in which it lowers the perceptions of security for our respondents. They showed that they are relying on the bank to compensate them in case of any security breach of private information or monetary loss where it was clearly shown in our findings where users discussed the fact that they are not worried a lot about security because they have the bank who supports the technology, and that they can with completing a for denying their responsibility of authenticating any transaction over the mobile banking they can get their money back. The study revealed also that banks assurances were a big source of initial trust for users of mobile banking technology where they were influenced by the bank to adopt the technology assuring doubtful customers about the downsides of using it. The type of assurances our respondent mentioned vary, some mentioned that they do not know about it while few others said that they received a statement from the banking when they adopted the service stating that the bank is supporting the service and that in case of any issue they can contact the bank’s customer service.

Our findings correspond with several studies in the literature around structural assurance. (McKnight et al 2011p. 12:7) stated that contracts, guarantees and other safeguards make success in trusting the technology more likely and (Kim et al 2009, p.290). The structural assurance in mobile banking include compensation of monetary loss due to service faults and breach of security, in addition to (Pennington et al 2003, p.201) where he assured that security statements provided by the trustor which is the bank in our context helps in building initial trust.
6.1.2 Propensity to trust

The findings of this study about users’ propensity to trust, and the level they rely on the general technology in their lives indicated that young users are relying to some degree on the mobile banking technology in their daily life and that it has proven to functional for them and that it added value to their life. This has decreased their security perceptions as they are more familiar with general technologies as they tried and used alternate methods of paying. The reasons of switching between various payments methods can vary between the general technology acceptance of the place they are in and their personal preference where some participants indicated that they sometimes just prefer to pay with older ways like cash and credit cards rather than using mobile payments, so this would reduce their usage of mobile banking. Their dependency on technology in general can be shown in other application or technologies such as social media applications like Facebook and Twitter, which made them more comfortable and faithful using the technology. The positive outcomes generated from using the mobile banking was expected by users to be in time and effort saving for them instead of the conventional ways, however few customers shown that they still prefer to use the conventional ways of banking.

Our findings are found in the literature in McKnight et al (2011, p.12:7) where they stated that individuals’ beliefs about attributes of information technologies in general and that positive outcomes will result from using that technology.

6.1.3 Trust in technology

Our study considered trust in the technology as part of the perception of security when using the mobile banking and in most of interviews users consider trust in the technology plays a big role in forming their attitudes and perceptions towards mobile banking security. Several aspects of the technology have proven to be important to them as they consider trust in the technology of mobile banking they are using to be added and aggregated with the trust in the banks themselves, the added value of the technology to users have been particularly impressing and may significantly impact their feelings of security.

The technology has proven to be very useful in many situations where it allowed them to access their bank 24 hours a day from everywhere they go, and provided them the ability to do transaction from the mobile phone in addition to perform mobile payments as well through connecting their bank account to their mobile number, while one of them indicated that the technology was not functioning properly which has led him to keep using the computer to perform different bank tasks, such as checking account balances, performing transactions, payments and so on forth. Looking in the literature, this confirms to (McKnight 2011, p.12:9) that users consider whether the technology delivers on the functionality promised by providing the features sets needed to complete a task and that the competence of a technology represent users’ expectations about the trustee’s capability.

Our users also indicated how helpful the application was and what kind of information and advice they found in the application, as they found all necessary information about how to reach the bank, and ask for any relevant information about student loans, or guidance about locations of ATM machines that the technology enables in addition to that the technology has a comprehensive guide about how to use it in case of any technical difficulty. The different related features provided by the application that are not only limited to payment but can complement the service were highlighted and described as helpful. In literature, this confirms the definition of technology helpfulness of (McKnight 2011, p.12:9) that technology offers a help function and will provide necessary advice to complete a task.
Our respondents shown that the technology is reliable for them, where they appreciate the fact that they need the technology in their usual daily lifestyle and that the technology is useful for them in today’s quick world, and that they require a service that is constantly running and available to serve their needs, however those who do not use the technology in most of their banking purposes shown that they still have doubts over the mobile banking and that they still prefer to use online banking from the computer instead due to some trust issues with the technology that are mostly related to the fact that the technology is still new for them and that they are not used to it. Our findings indicate then that, first: for those who use it often shown that it is reliable and useful for them, while those who do not use it stated that they still do not trust or familiar with the technology which generally confirms (McKnight et al 2011p.12:2) that reliability of the

6.2 Application Quality
Our study explored the effect of visual aspects on perceived security and revealed that the many participants thought that the design of the application affected their levels of trust and security perceptions. We found that several elements that are related to the quality of the application of mobile banking can play a role in security perceptions of users. The application design and layout can communicate a trustable and reliable platform that can even overcome the technical aspects of security for users where it indicates that the application is well invested in, in addition to the language where we found that when users engage in unfamiliar language applications they tend to be careful or minimize their uses of the service as they fear mistakes or errors that would lead to unwanted actions.

In the literature, it corresponds to (McKnight et al., 2002 p.341) where good information quality enhances users trust, and (Kim et al 2003) who stated that accuracy of information influences trust and behavioural intentions, in addition to (Corbitt et al., 2003, p.252) where site quality influences trust perceptions of the users. Therefore, attention and constantly updating the service design and look as well as content is necessary to maintain customers trust in mobile banking. Having negative designed application will cause users frustrations and gives the indication that the application lacks proper investment which also can be reflected on the perception of the security of the application. (Vijayasarathy, 2004, p.757) states that poorly designed interfaces, cluttered pages and layouts with poor information quality contribute to customer frustration. According to our results of the study it is clear that informing and educating customers about security information and threats needs to be implemented especially in mobile services. The poor knowledge of the user about information security contributes to lower perception of security and higher risk of attacks on the mobile banking service causing the customer to trust less the mobile banking application provider. Our participants indicated generally their low level of awareness and knowledge about information security of mobile banking stating that the warning signals they receive are not enough and that they prefer to receive more knowledge and information about security of the service.

6.3 Visible security mechanisms
The participants’ awareness of the security mechanisms in mobile banking was found to be low or weak on average, even though the IT students have relatively better knowledge about the technology however they shown that their general knowledge about security is somehow low. The main visible security mechanisms we found are related to three security objectives that are: authentication, authorization and privacy. These are the mechanisms that are mainly used and observed by the users during their usage of the mobile banking application. The mechanisms associated with the authentication objective include: usernames, passwords, personal codes, digital identification, biometrics and date of birth, while the ones associated
with the authentication objectives where mostly found to the use of confirmation codes and biometrics. For the privacy policy in the application it was found that the mechanism that explains the banks policy is found on the application on a separated page or window. It is worthy to note here that not all the banks have such option in regard to the privacy.

The perception of customers in general found to be in favour of combining more of these steps in logging in the application of mobile banking where our participants indicated that use of multiple was to log in the application can increase their sense of security, also customers prefer to use more and stronger authentication steps to confirm their transaction on mobile banking and having the privacy setting enabled and viewed on their mobile banking application, so they would know what information are being collected from them. For the other security mechanisms like non-repudiation, encryption, confidentiality and auditability were not mentioned by our participants, the mechanisms of integrity and availability are shown in other parts above that are related to trust in the service so we think that discussing them again in this section will not add to the thesis.

The findings in regard to visible security mechanisms correspond to (Chellappa & Pavlou, 2003, p. 361) where customers’ perceptions of security are influenced by the visible mechanisms, and that those perceptions are built upon the self-assessment of these technological mechanisms. The importance of visible security mechanisms was also discussed by other researchers as (Link et al., 2006, p.6) where objective security influences the subjective security as users named what they can see from security mechanisms. (Kim et al., 2010, p. 87) stated that users’ concerns include visible technical protections of the service. Users also stated their preference towards having multiple security options to log in when use the mobile banking, our finding on this matter corresponds to (Kim et al., 2010, p. 89) where more authentication assurance enhance the perceptions of security for mobile banking users.

6.2.1 Usage experience
In our study, we found that there is influence of past experience of usage of the mobile banking services whether in mobile banking or in m-commerce have a relation with the levels of security and trust perceptions of users, we found that in general usage experience can affect the security perception of mobile banking users but has low impact on that perception, this is due to the fact that the necessity of the service has can outcome the security perception. We found that the negative security experiences can cause stop or limit users from dealing with certain partners on m-commerce but not for example stop using the service of mobile banking, while the positive security experiences will increase the level of trust and positively impact the perceived security of the bank and its products in general. The effect of past experience has also been discussed in the literature by (Shin, 2010, p.88) where he stressed that customers may have different attitudes towards the security of internet services with regard to their requirements and that the positive effects of the user can impact perceived security.

6.2.2 Amount of transfer
We measured as well whether the amount of money kept in the account used in mobile banking or the amount of money transferred via the mobile banking channel matter to our respondents in terms of security perceptions of the channel. Our study revealed that for few users they would not transfer large amounts of money due to the fact that they prefer doing that on computer device because they perceive it as riskier, however due to the fact that our respondents are students and from young age they have no large amounts of transfer nor account balances so our result are more hypothetical in nature. The study also shows that users have some concerns in regard to putting all of their savings in an account stating that when they will have large amounts of money they will put them into separate account that has no internet access and leave relatively low amount of money to perform their mobile or
internet banking transactions. Our results contradict to (Goeke & Pousttchi, 2010, p.100) where he states that the payment does not generally have influence on perceived security while they correspond and confirm with (Bauer et al., 2005b, p.216) that transaction security is a major concern for users where users prefer to transact smaller and quick amount of money and are willing to accept lower level of security.

6.2.3 Device

Our study examined the perceptions of security and trust in terms of the type of device and how different devices with different software can affect the perceptions of security for our respondents. We found that users are worried about losing their device and that the ones who keep personal information and banking information have higher worries about security of their because their data are kept in their devices, we also found that few users give attention to the fact that the type of device can have different security. Our respondents mentioned that the software type and modifying the platform were the factors related to the type of device that can change their security perceptions, however we found a weak relationship with mobile banking as the type of device affects the security perceptions about the devices in the first hand. It is unlikely that it will cause a major effect on mobile banking.

In the literature, it was found that security mechanisms in mobile devices alter and may cause security concerns for the users (Coursaris & Hassanein, 2002, p.7) also the misuse and abuse of the mobile device can make it more vulnerable to security threats which in our case was changing the software and altering the platform of the device (Varadharjan, 2000, p.200).

6.2.4 Network and connectivity

Our study measured the effect of the type of internet connection on the perceptions of security and trust for our respondents and the results indicated that there is a notable effect between the type of network through which the mobile banking device is connected to the web. The finding showed that the cellular data is perceived generally safer than a wireless connection according to the respondents while public networks where the lowest in terms of security perceptions of the users. The study also showed that the security of each network and the number of people who are connected to the network played the role in forming the attitude towards avoiding connection with public and wireless networks, also the study shows that there could be a small impact of the stability of the connection on the security perception.

In the literature, our finding corresponds to (McKnight et al., 2012, p.12:7) where he stated that the situation in which the technology is being used determines the level of comfort and trust for users to use the technology, in addition to (Coursaris & Hassanein, 2002, p.12) who stated that users become concerned about the safety of the information transmitted over a wireless network as the degree of communication of sensitive information increases. Users when using mobile banking are sending sensitive information about their mobile banking accounts and what their devices also contain of information and they feel they might get hacked while using the service.

6.2.5 Familiarity

Our study explored the effects of how familiar our users with the technology of mobile banking on their trust and security perceptions in mobile banking technology. The results show that the majority of users felt insecure about the technology and service at the beginning of usage, however with more transactions made and familiarity with the way the mobile banking application works through what people are talking about and discussing in regard to this technology and how positively or negatively they describe their experiences, their trust levels changed and they became more familiar with the technology which removed part of their security concerns. Our respondents indicated that now and in the future, it is unlikely
that they will stop using the mobile banking unless a major security breach happen which means that they have now with the technology a good level of trust and dependability. In the literature, this is found in (Gefen, 2000, p.726) where he stated that people’s positive or negative opinions affect each other’s disposition to trust and intention to use and adopt…

6.2.6 Awareness of security threats
Our respondents shown different levels of knowledge and awareness about security threats that might affect their mobile banking experience which we consider in this context the awareness of the known which is the technical security threats that might affect the user and the counter measures they do to protect themselves from those threats. Such threats we found to be related to the hacking process where we found that users may be aware of some methods and scams that hackers use to obtain their information such as receiving unknown links and e-mails in addition to suspicious infected files that can be detected by the protection applications, where such threats result in several consequences that not only steal customers data but can affect the device and stored data and doing damage. The awareness of such threats and their outcomes can result in increasing perceptions of security and users become more careful when using their mobile banking applications. We found that the more people know about security threats more careful they are in using the application and where sceptic about the security of the application in certain situations such as being connected through the use of more difficult passwords, changing them often, avoiding connection to public networks, using passcode locks on their smartphones and preferring to have more security options and steps in their mobile banking.

The findings in this part confirm with (Komiak & Benbasat, 2004, p.196) in which awareness of the known has a relationship and influences the emotional side of trust where It has a relationship with their feelings of being secure and comfortable. The emotional trust is an attitude and in our context the users have shown an attitude and tendency to be safer due to their level of knowledge about possible negative consequences and the technicalities of hack and cybercrime (Komiak & Benbasat, 2006, p. 943), hence there is a relationship here between awareness of security threats and emotional trust where the type of relationship is negative in which more awareness about security threats leads to lower levels of emotions and feelings of comfort and security, also this finding corresponds with (Suh & Han, 2003, p.137) as customers when they do not understand security controls they wary about the security in the technology in addition to (Adams et al., 2005, p.338) where the lack of knowledge about security causes users to make errors and mistakes when using the technology, it is shown clearly when sometimes users mistakenly open unsecure messages or e-mails etc.

To summarize our analysis, we present a table with a summation of all the theories used in the study as we related to them in our theoretical background. These theories formed our themes and upon which we presented and analysed the data.

Table 7 Theories checked

<table>
<thead>
<tr>
<th>Theories</th>
<th>Researchers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Situation Normality</td>
<td>McKnight et al., 2002</td>
</tr>
<tr>
<td>Structural Assurance</td>
<td>McKnight et al., 2002</td>
</tr>
<tr>
<td>Faith in technology</td>
<td>McKnight et al., 2002</td>
</tr>
<tr>
<td>Trusting stance</td>
<td>McKnight et al., 2002</td>
</tr>
<tr>
<td>Reliability</td>
<td>McKnight et al., 2011</td>
</tr>
<tr>
<td>Functionality</td>
<td>McKnight et al., 2011</td>
</tr>
<tr>
<td>Category</td>
<td>Reference</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Helpfulness</td>
<td>McKnight et al., 2011</td>
</tr>
<tr>
<td>Emotional trust</td>
<td>Komiak &amp; Benbasat, 2006</td>
</tr>
<tr>
<td>Awareness of the known</td>
<td>Komiak &amp; Benbasat, 2004</td>
</tr>
<tr>
<td>Awareness of the unknown</td>
<td>Komiak &amp; Benbasat, 2004</td>
</tr>
<tr>
<td>Security mechanisms</td>
<td>Hutchinson &amp; Warren, 2003</td>
</tr>
<tr>
<td>Perceived security</td>
<td>Ally &amp; Toleman, 2005</td>
</tr>
<tr>
<td>User demographics</td>
<td>Shin, 2010</td>
</tr>
<tr>
<td>Information quality</td>
<td>(McKnight et al 2002)(Corbitt et al 2003)</td>
</tr>
<tr>
<td>Amount of transfer</td>
<td>Goeke &amp; Pousttchi, 2010</td>
</tr>
<tr>
<td>Type of device</td>
<td>Coursaris &amp; Hassanein, 2002</td>
</tr>
<tr>
<td>Type of network</td>
<td>Coursaris &amp; Hassanein, 2002</td>
</tr>
<tr>
<td>Communicating security</td>
<td>Linck et al., 2006</td>
</tr>
<tr>
<td>information</td>
<td></td>
</tr>
<tr>
<td>Usage experience</td>
<td>Shin et al., 2010</td>
</tr>
<tr>
<td>Familiarity</td>
<td>Gefen, 2000</td>
</tr>
</tbody>
</table>
Chapter 7: Conclusion

This chapter will present the final conclusions of the study in terms of the research questions and the main contributions. It will further present suggestions for future research, limitations and implications of our study.

7.1 Summary of results and analysis:

Aiming to get a better understanding of customers’ attitude towards mobile banking security and trust issues, we designed this research to interpret this phenomenon. To be specific, we generate two research questions from related theories. Our study aimed at reaching our objectives mentioned in the introduction and answering the research question and such objective make our research more directed. Thus, a qualitative research guided by interpretivist philosophy is conducted. By using interviews as our main data collection method, we are able to comprehend how people perceive mobile banking security and trust issues, and their opinions towards them. The research questions are about young mobile banking users’ perceptions of security and awareness of security threats and how it influences their trust in Mobile banking. Through this research, we summarize our findings in a way that answers our research questions, by listing the relevant themes we found and explaining how young mobile banking users perceive security in mobile banking according to each theme and theory.

How mobile banking young users perceive security in mobile banking?

To Our interviewees have shown several responses and factors that would make their perception of security, and trust in mobile banking technology and institutions has played a big part in forming the perception of security. We linked these factors to previous literature on electronic banking and payment systems, in addition to mobile usage. We found that guarantees and assurances of the banks play important role in securing the user in face of threats that would cause them to be hijacked such in case of lost money or suspicious transactions, users can still use the service with the bank promising them to compensate their loss and provide the necessary tools to prevent future crimes. Situation normality also was part of the feelings of security and comfort of the users where the surrounding environment, culture and people’s perceptions of the technology and the way the technology is being used. Our respondents shown that their perceptions of security are affected by their social circles and experiences of their friends, relatives and people they know, in addition to the security mechanisms themselves provided by banks to secure mobile banking applications which can be found in several logging options, the use of biometrics and code generators to complete transactions.

Faith and trust in technology in which young users are dependants on the technology in their daily life makes it difficult for them to replace which can reduce the security perceptions. Our respondents indicated that they rely on the technology in their life which can lead to less degree of security attention. The reliability and functionality of the application can affect the security perception, where having a functioning and reliable application leads to more trust in the technology and lower perceived security. Application quality: the language and design of the application can be more important indicator on the level of security than the security mechanisms themselves for users. Users might perceive a well-designed application is more secure because in their opinion it might indicate that the bank invested in the layout of the application and visuals to present it in a good way will indicate also that the bank invested in its security measures.

The usage experience, where positive and negative experiences of the user play a role in security perceptions. Our users indicated that when they experience more successful transactions with mobile banking they are more inclined to deal with it again, also the amount
of monetary involvement in either transacting through mobile banking or the current balance. When performing big transactions users tend to be more careful and try to take more security measures like being alone when performing it. The type and nature of the device used and its software related experience. The software IOS of Apple devices for example was found to be perceived more secure due to being closed system and users may be subject to more threats when jailbreak it and level of awareness of relevant technical security issues and security incidents communicated through the media. Stories and articles about security of mobile banking found online can play a role in shaping the security perceptions of mobile banking users and their awareness of how they might get hacked.

7.2 Main contributions
A considerable amount of the related research has explored the perceived security as a factor of trust, we considered both concepts as equal and have a direct relationship based on Kim et al., (2010) who examined security and trust from the view point of customers in electronic payments, such consideration of the study was helped in clarifying that both concepts affect each other. It incorporated the young users as a special context of the study because of their notable engagement of mobile banking applications based on Wijland et al., (2016) who concluded that young users were engaged in using mobile applications, hence we aimed to applied the theoretical concepts on mobile banking young users and produce our results. Our thesis explored the security and trust perceptions of mobile banking for young customers and indicated which ways are relevant to the topic discussed, and the complexity of items that play role in the security network for the users, however our study examined these perceptions in general without specifying the examination of any particular mechanisms or factors that play the role in forming and affecting such perceptions. It helps the reader in forming a comprehensive conception of the topic and the technology of mobile banking security that has not been widely covered in regard of the topics discussed, and has given a number of indications on the way users of mobile banking perceive the security in the technology which can be taken in account when designing and improving mobile banking applications. The theories we used as frame of reference correspond with the actual findings from our interviews, where our results are supported and embedded theoretically in the body of literature we found. Because we wrote about mobile banking as a technology, we relied in selecting our theories on the fact that it is considered a technology thus we based the paper on Mcknight et al. (2011) Trust in a specific technology which is not widely referred to in mobile banking literature, the same applies to Komiak & Benbasat (2004) study that also consider the cognitive side of trust as a feeling of security and comfort of the trustor, using which we linked the concepts of trust and perceived security and treated them as closely related in our study.

This study implies that managers of banks and mobile banking consider the level of knowledge of mobile banking users that may differ between generations and showed that mobile banking young customers have no problems using the service backed by the banks assurances and protections from fraud however, this might not be the case in regard to other age groups who have different understanding of the technology and security education. Also our study raises the importance of mobile threats as an increasing cyber threat given the relevant grow in its uses and services offered via this channel and calls for more attention and protection given to mobile applications and making users aware of that the level of security may differ between computers and mobile devices hence we encourage conducting further studies and pols on the matter.

7.3 Limitations of the study
This research is conducted under the instruction of qualitative paradigm. Therefore, it has some general limitation of qualitative research like it is too subjective, difficult to replicate,
problem of generalization, lack of transparency. Now we will consider those limitations within the context as well as particular limitations in our study.

There are several limitations to our study that we need to notice. First, under interpretivist philosophy we investigate our research not only by existing knowledge from literature but also the knowledge we have or our own experiences. That means the whole research involves our attitudes. We structure the interview questions by ourselves understanding of trust and security, we interpret the answers from respondents in our own way. This results in that our research may be too subjective. Considering the time consuming and cost, the geographical positions constraint restricts our research only conducted around Umeå, Sweden. In addition, the samples we chose are all students from Umeå University. That is to say, we only investigate certain customers from certain environment. They may have some similar cognition towards the topic we discuss. The limitations of territory and sample selected may lead to biases of result. If this research is conducted in other group of people from different country or different ages, the result may be different. The other limitation is, due to the number of respondents, our discussion of mobile banking security is very general. Since banks are the main services providers of mobile banking, they also play an important role when we investigate security and trust issues. We admit that the service quality, the security measures and other bank related issues will impact customers’ perception of security and their trust of the certain bank. In our study, we do not distinguish respondents from which banks they receive the services. In other word, this indicate that the result of our research can be only used in general situation. It does not take the differentiations of banks into consideration.

7.4 Truth criteria
The credibility of the results is an issue that must be addressed, hence the discussion regarding this in the following chapter. According to Saunders et al. (2009, p. 156) it is impossible to know if the evidence and conclusion of any study have been correctly understood. Therefore, what can be done is trying to reduce the risk of misinterpretation through a solid, well-thought research design, especially in two aspects, namely reliability and validity. Saunders et al. (2009, p. 156) Reliability, validity, and generalizability of the results will be discussed in this chapter.

7.4.1 Reliability
According to Bryman and Bell (2011), it states that reliability is a definition concerning about the measurement of the research. When researchers try to get a reliable result, the measurements they use, like practical methods or analysis method, should be accurate and precise. To demonstrate the reliability of the research, it requires the result of the research should be as little differences as possible. (Collis and Hussey, 2014, p. 52) We believe it assists us to gain a more reliable research result if all the processes of the research satisfy the requirements of reliability. Thus, we are able to ensure our research is meaningful and the contributions are worthy to discuss.

Bryman and Bell (2011, p.400) pointed out two main factors of reliability in qualitative research, which are external reliability and internal reliability (Bryman & Bell, 2011, p. 400). External reliability refers to the absence of differences when the research is repeated. But considering the characteristics of our research, we believe there are some existing difficulties leading to a less differences replicated research. One reason is, this research is conducted in a specific area (Umeå) and the respondents are within young generation. On account of economic development level, transportation services level, even the density of population is different from area to area, the result may be different if this research is conducted in another place. As we have discussed in chapter 4, younger generation are more willing to accept new born technologies, we also hold the view that research result will be different if we choose
people from any other ages as our sample. Moreover, within interpretivist paradigm acted as researchers who always take part in the research, using our own knowledge and life experience to analyse the data we collect, meaning that the result of interpretivist research is highly dependent on the researchers’ points of view because of the subjectivity of research, when it is repeated it is difficult to replicate a similar knowledge system like the researchers they have, which may cause totally different research results. As it has discussed in theoretical paragraph, we regard mobile banking as a competitive service provided by banks. We design this research on the basis of our study background as business students in marketing and accounting fields, and thus we kept the study away from technical terms as we could. The existing of different results are of high possibility if replicated research adopts any other knowledge or from other perspectives. Those listed two main reasons explain the external reliability issues of this research. Generally, in qualitative research external reliability is often hard to meet (Bryman & Bell, 2011, p. 400), but supposed that repeating the research as the original one does, which means, use similar methods to collect data, similar theories to analyse it, the differences in results could be reduced.

Internal reliability concerns about the consistency of inter observers. In our research, our respondents play the inter observer’s role. When scanning through the response of each interview, we find the correlation of answers in one interview shows a very high level. The reason can be the interview questions are not only followed by instruction, but also generated from respondent’s answers of previous questions. This indicates that our research has met the basic criteria of internal reliability.

7.4.2 Validity
Validity has been emphasized so much signification when evaluating a research. As Bryman (2012, p. 47) states, validity can be seen as the most important criterion of a research. To satisfy the requirement of validity, the result should be generated exactly from the research. In our research, with the purpose of demonstrating validity feature, we examine the theories we adopt to elaborate the investigation process and the research conclusions.

To make it easier to evaluate, Bryman (2012, p. 390) categorize two branches of validity. Internal validity calls for the good fit between data and theories. In theoretical chapter, we presented several theories and background about mobile banking, security and trust issues. Using those theories as instruction, we organized and structured interview questions by asking respondents their feeling and knowledge about those theories in specific environment. When we were doing data analysis procedure, we made sure to extract the most original information from those interviews. As a result, the consistency of observation and theoretical basis is successfully developed. Another branch is external validity, which emphasize the measurement of findings (Bryman, 2012, p. 390). A research which achieves external validity means that findings of this research are ready to be expanded to all different social phenomena (Bryman, 2012, p.390). This criterion is often not so easy to be satisfied especially in qualitative research. As we mentioned before, our investigation is established on particular area and young people. Therefore, the implications of our research may only have its certain meaning within specific context. There is a possibility that the result will differ from any given factors. In this regard, we shall recognize the external validity of this research is not as high as internal validity.

7.4.3 Generalizability
Generalizability is often referred to as if the results can be transferred to become the same if the study was reproduced at a later point in time. In quantitative studies generalizability is often related to whether or not the sample method was corrected and the population was presentable (Bryman, 2011, p. 168-169). Since we wanted to explore how young users are
perceiving security in mobile banking and its reflections on their trust in the technology, and that our study was done with relatively small sample and limited geographical area, we did not aim to draw any general conclusions. We hope that the knowledge and information explained in this study will help in raise attention towards this matter and help others who could be doing similar studies and researches, we wanted to draw a frame of understanding of the subject of mobile banking and security issues that surround this technology since this technology is subject of attention and the dependence on this technology is expected to increase in the future.

7.5 Future Research

This thesis explored perceived security and trust in mobile banking in general without specifying the examination of any particular mechanism of security solutions. The paper helped in forming more advanced knowledge and contribution to the subject that has not been widely studied before in terms of combining and relating both concepts of perceived security and trust. In the future, it would be appropriate to explore the topic further with the particular mechanisms we mentioned and identified their impact on perceived security of mobile banking, such as the impact of applying biometrics authentication techniques on customer security perception in mobile banking and perceived security. We also suggest exploring further the concept of awareness in the context electronic banking and examining the computer level of threats.

Future researchers can conduct an investigation through a wider geographical field therefore, they are able to reach different mobile banking users doing quantitative studies. We believe that different cultural background, different social developing phenomenon, different technology used in mobile banking can contribute to diverse perceptions of this topic. We also suggest conducting a similar research but from the banks perspective to examine how customers report them their level of satisfaction about the security measures applied in mobile banking, also measuring the size of costs that the banks incur due to compensating for any security breaches and the impact of that on the balance sheets of the banks.
Chapter 8: Ethical considerations

In this chapter, we report all the ethical considerations associated with our research. The chapter is structured according to each stage of the research. We start first with discussing the need to address research ethics, then we discuss it further in conducting the study, in data collection, reporting the findings and finally in analysing the data.

8.1 Why research ethics

David & Sutton (2011, p. 30) explain ethics term as a work or a collection of rules to examine how good or bad the research is conducted, while Saunders et al (2009, p. 183) explains that ethics are the level of appropriateness of the researcher’s behaviour in relation to the rights of those of become subjects to the work, it is therefore related to addressing issues and answering questions about how we formulated and clarified our research topic, gained access, how we collected, analysed and reported the data and wrote our thesis. As a supplementary part of the research we believe it has its own necessity, therefore we wanted to give it its own space of our work.

A research which is conducted in an ethical way can be easier to accept by others, and increasing its convincing and confidence, we conducted the research according to the Umeå university thesis manual and code of ethics. When discussing ethical issues in one research, to make it easier to understand, it is supposed to be ethical in every stage of the research (David & Sutton, 2011, p. 29) which means, we will demonstrate ethics term in both before the research, during the research, and after the research.

8.2 Before the research

Saunders et al., (2009, p. 188) explain that in designing the research there are issues associated with research ethics where the researchers have to adapt their research strategy to the choice of methods where is appropriate in addition to considering and planning how to gain access to participants. In this stage, we mainly address the philosophy we used in this research, as well as the associated ethical concerns with it in addition to addressing the process of how we gained access to our participants.

Interpretivism, as the philosophy we choose to use in this research, acting as the guidance of whole research design and construction. It shows a general direction of this research. An interpretivist research always focuses on people’s feeling or thinking about something. It also calls for researchers’ involvement when performing the research. Adopting this philosophy implies that our research not only investigate people’s behaviour or feeling, but also utilizing our own knowledge to analyse why they think or act in this way. We choose to investigate mobile banking under this philosophy because it is worthy to. We believe the value of our research it high. The data we gained the result we found, are all based on facts, and do contribute to real world and future study. Combine the knowledge we learnt from school courses and previous experiences with the phenomenon we observe in this research, it reaches a good fit between philosophy and practical outcomes. In this perspective, we believe we have embraced the ethical way in the decision to research.

For the issues related to negotiating access we addressed several factors in order to address the rights of our participants during the research process as individuals have the right to privacy and should not feel pressurised or coerced into participating (Saunders et al., 2009, p. 188).

8.3 During the research

In this stage, concerning ethics in practically conducting a research, David & Sutton (2011, p. 43) list three important principles to measure whether the research is conducted in ethical way
or not. They are: informed consent, protection from harm, and privacy (David & Sutton, 2011, p. 43). Collis & Hussey (2014, p. 31) also state several similar notions when testing the ethical level in a research, a research is deemed to be ethical in process if it meets all the notions’ requirement.

We narrow down this discussion to data collection paragraph, because this section is the only part which needs respondents take part in. Firstly, in the process of performing the research, it should not be harmful to research participants (Collis & Hussey, 2014, p. 31). Due to our interviews only ask about people’s perceptions and actions of mobile banking security and trust issues, it won’t involve in any physical harm to them obviously. Secondly, through the requirement of informed consent, participants should agree to play a part in this research, and be well informed about the content of research (Collis & Hussey, 2014, p. 31). In other words, they should be noticed what this research is about. Following this notion when we select samples, we make sure we have illustrated the research purpose and what we want them to help us very clearly on the recruiting notices. Despite that, before conducting each interview, we explain what the interview is about and ask their agreement to participate in it again. Those steps ensure every respondent understand the topic of our research, and they do really are willing to take a part in it. Therefore, we are able to satisfy informed consent. The third principle is to protect participants’ privacy from being invading (Collis & Hussey, 2014, p. 31). Considering mobile banking information is closely related to participants’ wealth security, and even may involve in their personal information like password or mobile number, we decide to not mention so much detailed questions about their private information. For example, any personal information won’t appear in data collection process, like their name, birthday, from which bank they get the mobile banking service and how much money they deposit in that bank account. In some situations, we have to inquiry their own experience when using mobile banking (especially some negative attitude towards the bank which provides them services), we keep those data secretly, not invade to any third parties. To make the research data safer, we will dispose all interview records and transcripts after finish this study. We ourselves as researchers, we also keep in mind that we should not cheat participants or lie to them to guarantee no deception principle. After checking these three principles, we believe this research shows a great respect to participants. Their privacy is successfully protected.

8.4 After the research
The final stage stresses that the ethics of form and use of findings need to be considered as well (David & Sutton, 2011, p. 50). We conclude what we find from data analysis procedure. As we have discussed above, we have made sure the research processes do obey with ethical principles. Those means the research findings also meet informed consent, protection from harm and privacy requirement. We realize that our study, as a degree thesis, will be exposed to public. The findings of our research also have the possibility to be used by banks or any other associations. What they will deal with the research findings, or even the original data of our research, is out of our control. This emphasizes our responsibility to protect respondents’ personal information.

Generally speaking, ethical concerns could be a core issue to be address in qualitative research if the researchers do not examine it carefully. Because qualitative researches always involve in people’s feeling and thinking towards something, their personal information is more exposed in the research. Especially in our research, the topic of mobile banking often linked to transaction like online payment or money transferring. To keep our research conducting in an ethical way, we come up with several methods to protect their private
information. Through them we are able to guarantee the security of the research and its participants. In all, we believe our research is conducted in an ethical way.
Reference list


Garrett, J. J. (2010). *Elements of user experience, the: user-centered design for the web and beyond*. Pearson Education.


Harris, L. C., & Goode, M. M. (2004). The four levels of loyalty and the pivotal role of trust: a study of online service dynamics. *Journal of retailing, 80*(2), 139-158.


### Appendix

Table: Literature review on Trust.

<table>
<thead>
<tr>
<th>Object of trust</th>
<th>Trust attributes</th>
<th>Type of Trust</th>
<th>Empirical relationships</th>
<th>Studies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human</td>
<td>Structural assurances, situational normality</td>
<td>Initial</td>
<td>Beliefs that outcomes are likely to be successful due to the presence of supportive situations and structures</td>
<td>McKnight et al., 1998</td>
</tr>
<tr>
<td>Human</td>
<td>-Protective legal or technological structures</td>
<td>Initial</td>
<td>-Institutional-based trust affects trust in vendor.</td>
<td>McKnight et al., 2002</td>
</tr>
<tr>
<td>Technology</td>
<td>Information quality, good interface design</td>
<td>Initial</td>
<td>-Perceived site quality aids formation of trust in vendor</td>
<td>Pennington et al., 2003</td>
</tr>
<tr>
<td>Human</td>
<td>Situational normality, structural assurances</td>
<td>Initial</td>
<td>System trust affects trust in vendor.</td>
<td>Pavlou and Gefen, 2004</td>
</tr>
<tr>
<td>Human</td>
<td>Feedback mechanisms, escrow services, credit card guarantees</td>
<td>Initial</td>
<td>Effectiveness of institutional mechanisms affects trust in the community of sellers.</td>
<td>Pavlou and Gefen, 2004</td>
</tr>
<tr>
<td>Human</td>
<td>Structural assurances</td>
<td>Initial</td>
<td>Structural assurances influence trust in mobile banking</td>
<td>Kim et al. 2009</td>
</tr>
<tr>
<td>Technology</td>
<td>Site quality, technical trustworthiness</td>
<td>Initial</td>
<td>Perceived technical trustworthiness and perceived site quality affects trust in web vendor</td>
<td>Corbitt et al., 2003</td>
</tr>
<tr>
<td>Technology</td>
<td>Competence, benevolence, integrity</td>
<td>Initial</td>
<td>Trust in e-commerce environment mediates the</td>
<td>Suh and Han, 2003</td>
</tr>
<tr>
<td>Technology</td>
<td>Description</td>
<td>Type</td>
<td>Description</td>
<td>Source</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Technology</td>
<td>Correctness, availability, reliability, security, survivability</td>
<td>Initial</td>
<td>Trust in e-channel influences adoption of e-banking</td>
<td>Kim and Prabhakar, 2004</td>
</tr>
<tr>
<td>Technology</td>
<td>Competence, benevolence, and integrity</td>
<td>Initial</td>
<td>Trust in recommendation agent influences intention to adopt and PU</td>
<td>Wang and Benbasat, 2005</td>
</tr>
<tr>
<td>Technology</td>
<td>Cognitive: Integrity, competence Emotional: feelings of security and comfort</td>
<td>Initial</td>
<td>Cognitive trust influences emotional trust (toward the behavior), which influences intention to adopt online recommendation agent</td>
<td>Komiak and Benbasat, 2006</td>
</tr>
<tr>
<td>Technology</td>
<td>Predictability, reliability, utility</td>
<td>Knowledge</td>
<td>Trust in technology solution affects perceptions of supply chain technology and long-term interaction between supply chain partners.</td>
<td>Lippert, 2007</td>
</tr>
<tr>
<td>Technology</td>
<td>Accuracy, reliability, safety</td>
<td>Initial</td>
<td>Initial trust in mobile banking influences behavioral intentions</td>
<td>Kim et al. 2009</td>
</tr>
<tr>
<td>Technology</td>
<td>Functionality, dependability, helpfulness</td>
<td>Knowledge</td>
<td>Trust in IT influences PU and PEOU</td>
<td>Thatcher et al., 2011</td>
</tr>
<tr>
<td>Human- Online</td>
<td>Ability,</td>
<td>Initial</td>
<td>Trust in vendor</td>
<td>Lee &amp; Turban,</td>
</tr>
<tr>
<td>Vendor</td>
<td>Characteristics</td>
<td>Knowledge Level</td>
<td>Description</td>
<td>References</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Human-Online Vendor</td>
<td>Ability, integrity, benevolence of an identifiable population</td>
<td>Knowledge</td>
<td>Trust in a community of sellers determines transaction intentions</td>
<td>Pavlou &amp; Gefen, 2004</td>
</tr>
</tbody>
</table>
| Human-Online Vendor    | **Cognitive:** Competence, benevolence, integrity, predictability  
|                        | **Emotional:** feelings of security and comfort       | Knowledge       | Trust in the intermediary, and trust in the community of buyers influences sellers’ intentions to use an e-marketplace again | Sun, 2010                                      |
| Human-Online Vendor    | **Trusting attitude:** a willingness to rely on a web vendor  
|                        | **Trusting beliefs:** ability, integrity, benevolence | Initial         | The influence of trusting beliefs in a web vendor on intentions is fully mediated by trusting attitude | Benamati et al., 2010                          |
| Human-Online Vendor    | **Cognitive:** Competence, benevolence, integrity  
|                        | **Emotional:** Feelings of security and comfort       | Knowledge       | Awareness of the known and the unknown, influences trust in e-commerce.     | Komiak & Benbasat 2004                         |

(or agent of the vendor) affects intention to use the technology  
Bhattacherjee 2002; McKnight et al., 2002; Gefen et al., 2003; Kim, 2008; Vance et al., 2008

Human-Online Vendor

| Cognitive: Competence, benevolence, integrity, predictability  
| Emotional: feelings of security and comfort

Trust in a community of sellers determines transaction intentions  
Pavlou & Gefen, 2004

Trust in the intermediary, and trust in the community of buyers influences sellers’ intentions to use an e-marketplace again  
Sun, 2010

The influence of trusting beliefs in a web vendor on intentions is fully mediated by trusting attitude  
Benamati et al., 2010

Awareness of the known and the unknown, influences trust in e-commerce.  
Komiak & Benbasat 2004