Mobile Payment in Saudi Arabia

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Sciences in Software Engineering

At the College of Computer & Information Sciences

At Prince Sultan University

By Abdulaziz Sulaiman Abanmi

May 2015
Acknowledgments

I would like to acknowledge and thank all the people who have contributed to this thesis and mainly the following:

- Dr. Mohammad Zarour for his guidance and support throughout the course of developing this master thesis starting from the day of discussing the subject until the very last minute of discussion.

- My parents for their prayers and continuous support.

- My wife for her patience, believe and unquestionable support since the beginning of the master program.

- My line managers and my dear friends for their continuous care and support.
Abstract

Payments in general have experienced a tremendous evolution in the last few years where payment industry has adopted the chip technology as an alternative to the unsecure magnetic stripe in the payment cards. The chip technology in payments is based on the EMV Integrated Circuit Card Specifications which was named after original organizations that created the specification, Europay, MasterCard and Visa. The adaptation of chip technology has opened the door for more advanced payment methods leveraging on the technical aspect of the EMV including mobile payments.

Mobile payment implementations around the world have experienced different results from a very successful story to failures due to different reasons. Studying those implementations will help in building the most practical architectural framework for mobile payment application in the Saudi market. In order to achieve that, this thesis is meant to identify the most successful and widely adopted technologies in mobile payments and understand the main factors deriving those solutions by analyzing the published work in mobile payments following a standard systematic literature review (SLR) and understanding the current payment ecosystem in Saudi Arabia.

Based on the conducted SLR and the uniqueness of the Saudi payment market which is clearly noticed due to the fact that all point-of-sale terminals are connected and managed by the central bank of Saudi Arabia (SAMA), an architectural framework for mobile payment application was suggested leveraging the suggestions of the ISO 42010 standard and considering the impact of the non-functional requirements (NFR) identified during the study.

This thesis focuses in proposing an architectural framework for mobile payment application tailored for the Saudi market by identifying first the success factors from different mobile payment solutions globally and the proposed solutions as well as technologies in those implementations using systematic literature review, second step was studying the existing Saudi payment systems and the overall payment ecosystem in the country, third step was reviewing known mobile payment solutions in the market to benefit from their experience and successful models – if any -, finally proposing an application framework that can be utilized by any interested party to implement a mobile payment solution for the Saudi market and this is, up to our knowledge, is not studied yet.
شهدت المدفوعات في صورتها العامة تطورا هائلا في السنوات القليلة الماضية حيث تبنت الشركات المصنعة والعاملة في نظم الدفع تقنيولوجيا جديدة تعتمدت على الرقائق المغناطيسية أو ما يعرف بالشرائح كبدائل للشرائح المغناطيسية غير الآمن في بطاقات الدفع.

تعمد هذه التقنية على الموانع المحددة في نظام الدوائر المتزامنة الذي تم وضعه بمساعدة كبرى شركات المدفوعات العالمية مثل فيزا وماستركارد وما كان يعرف سابقا ببيرو باي. فتح تقنيته مجالاً أوباً لمزيد من وسائل الدفع ليكون ذلك الدفع عبر الهواتف الجوال أو المتنقلة.

تطبيقات الدفع بواسطة الهواتف المتنقلة حول العالم شهدت نتائج مختلفة ما بين ناجحة جدا وأخرى أقل نجاحا لأسباب مختلفة. دراسة هذه التطبيقات المختلفة تساعد في بناء الإطار الأكثر عملية لتطبيق الدفع بواسطة الهواتف المتنقلة عامة وفي السوق السعودي.

من أجل تحقيق ذلك، فإن هذه الرسالة درست مختلف التقنيات الأكثر نجاحا والتي اعتمدت على نطاق واسع في الدفع عبر الهاتف المحمول كوسيلة لتفادي العوامل الرئيسية التي ساعدت على نجاح هذه التجارب ومن ثم اشتقاق الحلول الأكثر ملاءمة للسوق المحلي وذلك من خلال تحليل الأعمال المنتشرة في الدفع عبر الهواتف المتنقلة وفهم النظام المحلي للدفع في المملكة العربية السعودية وذلك اعتمادا على خطوات المراجعة العلمية المنهجية وبناءها على الدراسة العلمية المستفيدة والتجارب الفردية للسوق السعودي، تم اقتراح الإطار التقني العام لتطبيق الدفع بواسطة الهواتف المتنقلة اعتمادا على مقتراحات معيار الأيزو 42010 وبالأخذ في الاعتبار تأثير المتطلبات الغير وظيفية التي تم تحديدها في الدراسة.

تم اتباع خطوات محددة في هذه الرسالة للوصول إلى اقتراح إطار عام للدفع بواسطة الهواتف المتنقلة مصمم خصيصا للسوق السعودي من خلال تحديد أول عوامل النجاح من مختلف حلول الدفع بواسطة الهواتف المتنقلة عالميا والحول المرجح وكذلك التقنيات في تلك التطبيقات باستخدام الدراسة العلمية المستفيدة، وكانت الخطوة الثانية دراسة نظم الدفع المعروفة بواسطة الهواتف المتنقلة في السوق والاستفادة من خبراتهم والنموذج الناجح.

إن وجدت - واخيرا اقتراح الإطار النهائي الذي يمكن استخدامه من قبل أي طرف مهتم لتنفيذ حل الدفع بواسطة الهواتف المتنقلة للسوق السعودي وهو الأمر الذي لم يدرس بعد على حد علمنا.
## Contents

Acknowledgments .......................................................................................................................... 1

Abstract ......................................................................................................................................... 2

ملخص ..................................................................................................................................... 3

List of Figures 7

List of Tables 8

List of Abbreviations ...................................................................................................................... 9

Chapter 1. Introduction .................................................................................................................. 10

1.1 Introduction: ............................................................................................................................. 11

1.2 Background and motivations: .................................................................................................. 13

1.3 Problem Statement: ................................................................................................................ 14

1.4 Objectives: ............................................................................................................................... 14

1.5 Research Scope: ...................................................................................................................... 15

1.6 Main Contribution: .................................................................................................................. 15

1.7 Thesis Overview: ...................................................................................................................... 16

Chapter 2. Research Methodology ................................................................................................ 17

2.1 Introduction: ............................................................................................................................. 18

2.2 Methodology: .......................................................................................................................... 18

2.2.1 Conducting Systematic literature review: ............................................................................ 18

2.2.2 Analyze the data: ................................................................................................................ 19

2.2.3 Analyze the current payment landscape in Saudi Arabia: .................................................... 19

2.2.4 Develop the proposed architectural framework: ................................................................. 19

Chapter 3. Systematic Literature Review (SLR) ........................................................................... 21

3.1 Introduction: ............................................................................................................................. 22

3.2 SLR Process: ............................................................................................................................ 23

3.3 SLR for Mobile Payment .......................................................................................................... 26

3.3.1 Planning the Review .......................................................................................................... 26

i. The need for a review: .............................................................................................................. 26

ii. Research Questions: ............................................................................................................... 26

iii. Review Protocol: ................................................................................................................... 26

a. Identification of Research: ...................................................................................................... 27

b. Selection of Primary Studies: ................................................................................................. 28

c. Study Quality Assessment: .................................................................................................... 28

d. Data Extraction and Monitoring: ........................................................................................... 28
Mobile Payment in Saudi Arabia

Chapter 3. Security/Privacy...

3.3.2 Conducting the Review
3.4 Data Synthesis:
3.4.1 Security/Privacy:
3.4.2 Performance:
3.4.3 Interoperability:
3.4.4 Simplicity/Usability:
3.4.5 Cost Effectiveness:
3.4.6 Acceptance:
3.5 Mobile payment solutions (based on the SLR):
3.5.1 NFC-based Solution:
3.5.2 Biometric-based solution:
3.5.3 Barcode-based solution:
3.5.4 Cloud-based solution:
3.5.5 Solutions vs. Challenges:
3.6 Conclusion:
3.7 SLR Validity Threats:

Chapter 4. Real-life examples of Mobile Payment Implementations

4.1 Introduction:
4.2 Starbucks Mobile Payment Solution:
4.3 Google Wallet:
4.4 LoopPay Wallet:
4.5 Softcard:
4.6 Apple Pay:
4.7 Google Wallet vs. Apple Pay:

Chapter 5. Payments in Saudi Arabia

5.1 Introduction:
5.2 Cashless Payment:
5.3 Payment Systems:
5.3.1 SARIE: 60
5.3.2 SPAN: 61
5.3.2.1 Type of transactions:
5.3.2.2 Technical Design:
5.3.3 SADAD:
5.3.3.1 Type of transactions:
List of Figures

Figure 3.1: SLR Process in Nutshell: .................................................................26
Figure 3.2: Percentage of Mobile Payment Success Factors discussed in the selected papers: ..........32
Figure 3.3: 2D-barcode solution to overcome the security issue .............................................33
Figure 3.4: A cloud-based with QR-codes solution to address the security issue .....................34
Figure 3.5: Interoperable mobile payment solution ................................................................37
Figure 3.6: Technologies used during payment in mobile payment systems ............................39
Figure 3.7: Technologies used during authentication in mobile payment systems ...................40
Figure 3.8: SLR Papers / Country ...............................................................................41
Figure 3.9: SLR Papers / Source ..................................................................................41
Figure 3.10: NFC-Micro SD Solution ..............................................................................44
Figure 3.11: The payment model using 2D-barcode ..............................................................47
Figure 3.12: Proposed solution for cloud-based NFC payment system ..................................47
Figure 3.13: Mobile Payment solution factors ......................................................................51
Figure 5.1: ATM transactions in the SPAN network ............................................................62
Figure 5.2: POS transactions in the SPAN network ...............................................................62
Figure 5.3: SADAD model (www.sadad.com) ....................................................................63
Figure 6.1: Operational View for the interoperability concern ............................................69
Figure 6.2: SPAN Wallet – enrollment and provisioning of the service .................................73
Figure 6.3: SPAN Wallet Server .....................................................................................74
Figure 6.4: Enrollment Process .........................................................................................76
Figure 6.5: Enrollment sequence diagram ............................................................................76
Figure 6.6: Activation Process ...........................................................................................77
Figure 6.7: Sequence diagram for activation .......................................................................78
Figure 6.8: Payment context diagram ................................................................................78
Figure 6.9: Sequence diagram for payment .........................................................................79
Figure 6.10: SPAN Wallet Framework (High-Level) ............................................................81
Figure 6.11: SPAN Wallet Framework (Mobile Wallet App) ................................................82
Figure 6.12: SPAN Wallet Framework (SPAN Wallet Server) ............................................84
List of Tables

Table 3.1: Main search strings .............................................................................................................28
Table 3.2: Quality Assessment .............................................................................................................30
Table 3.3: Success factors in implementing mobile payment solutions ..............................................31
Table 4.1: Google Wallet vs. Apple Pay ...............................................................................................58
Table 6.1: Association of stakeholders to concerns ...........................................................................69
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMV</td>
<td>Europay, Mastercard and VISA</td>
</tr>
<tr>
<td>NFR</td>
<td>Non-Functional Requirements</td>
</tr>
<tr>
<td>SLR</td>
<td>Systematic Literature Review</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>ATM</td>
<td>Automatic Teller Machine</td>
</tr>
<tr>
<td>POS</td>
<td>Point Of Sale</td>
</tr>
<tr>
<td>CITC</td>
<td>Communication and Information Technology Commission</td>
</tr>
<tr>
<td>OTP</td>
<td>One-Time Password</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>SAMAMA</td>
<td>Saudi Arabian Monetary Agency</td>
</tr>
<tr>
<td>SPAN</td>
<td>Saudi Payment Network</td>
</tr>
<tr>
<td>SADAD</td>
<td>Electronic Bill Presentment and Payment System</td>
</tr>
<tr>
<td>EBSE</td>
<td>Evidenced-Based Software Engineering</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>ACM</td>
<td>Association for Computing Machinery</td>
</tr>
<tr>
<td>NFC</td>
<td>Near-Field Communication</td>
</tr>
<tr>
<td>FPT</td>
<td>Finger Print Template</td>
</tr>
<tr>
<td>QR-codes</td>
<td>Quick Reference Codes</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity number</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data rates for GSM Evolution</td>
</tr>
<tr>
<td>3G</td>
<td>Third Generation</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Network</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>USSD</td>
<td>Unstructured Supplementary Services Data</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>SARIE</td>
<td>Saudi Arabian Riyal Inter-Bank Express system</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction
1.1 Introduction:

Payments in general have experienced a tremendous evolution in the last few years where payment industry has adopted the chip technology as an alternative to the unsecure magnetic stripe in the payment cards. The chip technology in payments is based on the EMV Integrated Circuit Card Specifications which was named after original organizations that created the specification, Euro-pay, MasterCard and Visa (EMV) [1]. The adaptation of chip technology has opened the door for more advanced payment methods leveraging on the technical aspect of the EMV.

As a result of the advancement in the mobile technologies and the increase usage of smart phones, mobile phones generally have been identified as a candidate method for payment and an excellent successor of the payment cards considering the fact that people will tend to carry their mobile devices everywhere unlike their wallets.

The desire of paying using mobile phones has been challenged by the security concern surrounding those payments; hence the need of adopting a new secure way of enabling payments using mobiles is required without ignoring the different market players affected by this change, i.e. banks, card issuers, acquirers, merchants and definitely the mobile network operators (MNO) as a new player in this domain.

However, in order for us to have clear scope of the intended study, we need to clarify main definitions related to mobiles and financial transactions including mobile transactions, mobile payments and mobile banking as per to [2].

- **Mobile transaction**: refers to any transaction that is completed using mobile devices whether it is financial or not.
- Mobile banking: it can be referred to as a banking channel where the bank enables its financial services linked to the customer account via mobile channel.
- Mobile payment: includes the financial payments that are completed using mobile devices with many different models implemented globally that might or might not include the telecommunication networks.

Based on the above we can clearly define the mobile payment as the “transaction in which a mobile device is used to initiate, authorize and confirm an exchange of financial value in return
for goods and services.” [3], or “payments for which the payment data and the payment instruction are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device” [4].

Mobile payments can be classified based on one of the following aspects [5]:

- **Business model:**

  This category includes how the mobile payment implementation will be managed.

  Examples of that could be the following models:

  - Phone carrier independent: the implementation of mobile payment does not depend on a specific mobile network operator which gives the customer the freedom to use the service despite the mobile network he/she is using for mobile services.
  - Collaborative model: it is represented by the model that includes the main players from the financial sector such as banks as well as the mobile network operators in a joint-effort implementation?
  - Third operation model: presented by having a new joiner to the payment industry other than banks and mobile operators such as a governmental body or a regulator entity.

- **Technology used:**

  The technical implementation can be used in classifying mobile payments based on the way the payment is conducted which could be instant messaging (SMS), mobile web payment (WAP), or radio frequency such as NFC or Bluetooth.

- **User location:**

  User location while conducting the payment can be a way of categorizing mobile payments into local transaction at physical stores or remote transactions.

- **Security and reliability:**

  The implementation of mobile payment follows different levels of security measurements during the authentication and transaction, those levels can be classified into five different levels of security as seen below:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Basic with no security.</td>
</tr>
<tr>
<td>1</td>
<td>Password.</td>
</tr>
<tr>
<td>2</td>
<td>Digital certificate.</td>
</tr>
<tr>
<td>3</td>
<td>Smart card/chip card</td>
</tr>
<tr>
<td>4</td>
<td>Context-sensitive location.</td>
</tr>
<tr>
<td>5</td>
<td>Biometrics.</td>
</tr>
</tbody>
</table>
Accordingly, future mobile payment implementation should support any payment type performed by anyone, with any device, anytime and anywhere [5].

An important aspect of the mobile payment implementation is identifying the main stakeholders and their contribution. There are three groups of mobile payment stakeholders: providers, merchant, and consumers. However, more detailed classification of stakeholders can be considered as per to [6], and those are: Supervisor (such as government entity managing and governing the payment rules), Technology Provider, Financial Institutions (banks and card issuers), Mobile Operator, Third-party payment service provider, Merchant and User. Each of these stakeholders usually influences the decision of which solution or technology to be used and adopted as the best practice under specific circumstances [4].

Mobile payments have an advantage over regular payments especially in the micro-payment area which involves low value amounts [7]; however mobile payment success factors are still not clearly identified based on the reviewed papers where none of the reviewed papers have listed a set of factors claiming that those factors are the main drivers of the implementation, instead most of the reviewed papers have highlighted only few important factors based on their analysis. As an example, mobile payments in China was reviewed from all perspectives and the authors in [7] have found that improving efficiency and saving the customer’s time while performing the transaction are the main drivers in addition to the ease of use. All these factors are challenged by the security and interoperability of the solution which are yet to be resolved [7].

1.2 Background and motivations:

The total number of mobile users in Saudi Arabia has reached 51 million subscriptions with penetration rate of 169.7% [8]. This high utilization of mobile phone services has led to rank Saudi Arabia as the ninth country globally in mobile phone usage [9].

The continuous increase usage of mobile phones in Saudi Arabia as reported by CITC was not ignored by the banking industry in Saudi Arabia; instead all banks have reacted to this development by introducing mobile applications to their customers to be used for most of the fundamental services usually provided by the bank’s website. In addition to the traditional transactions supported by the mobile apps, most of the banks have provided access to important information to their customers via the mobile app leveraging the technology supported by mobiles including geographical location identification capability, those added-value services included the location of the nearest branch or ATM and the identification of special offers available close to where the customers are.

The introduction of mobile app is not the only indication of the attention given by Saudi banks to the fact that customers are attached to their mobile phones, this introduction of the mobile app service was preceded by the full utilization of SMS service (Short Messaging Service) supported by all mobile phones to deliver alert messages - helped to prevent fraudulent
activities – and communicating One Time Password (OTP) to the customer to be used for secure login and transaction completion which has increased the dependency on mobile phones as a way of providing financial services by Saudi banks.

Considering the increase usage of mobile phones in Saudi Arabia and the current age of “do-it-all devices” as well as the clear readiness of the local ICT (Information Communication Technology) infrastructure, it has become necessary to look into completing this experience and package of supported functionality and proposed payment solution in the market to leverage the advantages of mobile payment by enabling mobile phones to be a trusted payment instrument.

In addition to the above, the current setup of the payment systems in Saudi Arabia where all point-of-sales (POS) are directly connected to the payment network managed by the central bank of Saudi Arabia (Saudi Arabian Monetary Agency) is main driver to design a proper framework that consider this unique setup of the Saudi ecosystem and not to ignore the main role that SAMA or the central bank is currently playing in the payment arena.

It is also worth mentioning that although mobile payment implementations already exist globally, however a ready-made framework might not be available as most of those successful implementations are tailored for payment environments that are less governed by the regulations which make it easier to adopt any of-the-shelve product.

1.3 Problem Statement:

Mobile payment is, relatively, a new topic with various publications that discuss its concept, implementation as well as different experiences gained via case studies. Studies that make use of the available research in this domain to identify main issues that affect the success of mobile payment are very few. Moreover, mobile payment has not yet been implemented in Saudi Arabia with expectations that such implementation will need to be built on top of a contactless-enabled environment to facilitate the adoption of mobile payment implementation. This research work conducts systematic literature review to explore the main success factors and techniques to implement mobile payment and propose an architectural framework for mobile payment application in Saudi Arabia based on the available local environment in the Kingdom.

1.4 Objectives:

The main objectives of this thesis are:

- Understand mobile payment technologies.
- Conduct a systematic literature review to identify the main drivers of successful implementation of mobile payment application.
- Review examples of global implementations of mobile payment applications.
- Understand the technical setup for payments locally.
- Propose an architectural framework for mobile payment applications in Saudi Arabia considering the local setup and global trends.

1.5 **Research Scope:**

This thesis is meant to provide a clear view of the current implementation of mobile payment globally and then focus on the local payment ecosystem to finally propose an architectural framework for mobile payment application in Saudi Arabia that takes into consideration the technical challenges identified in the literature review as well as the local infrastructure and regulations to ensure smooth implementation of the service locally. The first part of the thesis is based on evidence-based software engineering to explore the available evidences that identify the success factors of mobile payment implementation. The literature review is conducted systematically as proposed in the EBSE discipline (see Chapter 3). The second part of the thesis studies the different approaches for mobile payment implementation then proposes an architectural framework for mobile payment application in Saudi Arabia. The architectural framework is based on the standard ISO/IEC/IEEE 42010 – Systems and Software Engineering – Architecture Description, and is depicted using UML deployment diagrams.

1.6 **Main Contribution:**

Payments is a key player in our daily lives, whether buying goods in-store or online. Simplifying those daily transactions for customers while introducing a better experience leveraging the new technologies is a real challenge. Hence, considering the current research trends in software engineering focusing on mobility and the continuous increase in mobile usage penetration, a mobile payment application should address the main requirements to convert the payment methods from the current traditional ways to a new and advanced one.

This thesis focuses in proposing an architectural framework for mobile payment application tailored for the Saudi market and taking into consideration the latest technologies, trends and success factors of mobile payment implementations globally.

The proposed application framework can be utilized by any interested party to implement a mobile payment solution for the Saudi market and this is, up to our knowledge, is not studied yet.

A research paper is currently in progress: *Mobile Payments: A Systematic Literature Review.*
1.7 Thesis Overview:

This thesis consists of six chapters discussing the main subjects around mobile payment solutions, local and global implementations.

Chapter 2 will cover the research methodology with brief sections discussing the main stages of systematic literature review, data gathering and application framework development.

Chapter 3 will provide a detailed systematic literature review (SLR) depending on the guidelines proposed for software engineering and provided by [10]. In this chapter, a detailed explanation of the used SLR process will be provided along with a detailed SLR in mobile payments in order to understand the main success factors and the used technologies to implement mobile payment solutions globally.

This chapter identifies how mobiles can be used to conduct payments, and what different approaches are available to make a successful mobile payment solution.

Chapter 4 studies real-life examples are discussed that illustrate the use of mobile payment implementations with details highlighting the technologies used by each solution. This study will help in adopting proven solutions – if any – or at least provide insights into the current technologies in real-life scenarios.

Chapter 5 will be dedicated to understand the payment infrastructure and ecosystem in Saudi Arabia to evaluate the possibility of integrating a mobile payment application and the main challenges preventing this implementation including the interaction with the main Saudi payment arms of the local central bank (Saudi Arabian Monetary Agency), i.e. SPAN (Saudi Payment Network) and SADAD (local bill presentment and payment) and conducting a quick interview with their executives.

Chapter 6 is the mobile payment application framework for the Saudi market that will take into consideration the outcome of all the previous chapters and present a technical application framework that can be utilized by any interested party to implement a mobile payment solution in the Saudi market with the minimum integration efforts.

Finally, Chapter 7 is covering the conclusion and future work, where a detailed analysis for all the different viewpoints of the proposed solution including information, development, deployment and functional viewpoints could be considered as an extension of this work in order to have more detailed understanding of the overall architectural framework of all system components. Also the limitations were discussed in this chapter including the security of the transaction and the possibility of attempting a successful fraudulent payment other than the addressed in this thesis, and finally the possibility of supporting offline transactions for better customer experience.
Chapter 2. Research Methodology
2.1 Introduction:

The systematic literature review helps in identifying the best evidences published in the literature that are related to a certain topic in software engineering. This field of study is commonly known as Evidence-based Software Engineering (EBSE). EBSE is usually targeting taking decision regarding software development by combining up-to-date best evidences from research with practical experience [11]. EBSE doesn’t enforce one-for-all solution; instead it promotes the most suitable and expected to succeed solution based on the situation and circumstances of the environment where the suggested solution will be implemented [11].

In the case of EBSE, the software engineering shouldn’t depend mainly on lab results and it should encourage gathering evidences from real-life projects, observations and surveys [11]. Therefore, EBSE is integrated within this SLR to achieve the main steps listed below and suggested by [11]:

- Convert the problem into a question.
- Search for the best evidence.
- Assess and evaluate the evidence to ensure its validity and applicability.
- Integrate the identified evidences with the practical experience and customer’s expectations along with the circumstances in order to take the right decision.
- Evaluate the final solution and provide improvement suggestions.

In order to achieve the main objective of answering the research questions, this research will follow the research methodology depicted by the below steps and figure 2.1 based on the need and the research question addressed in each stage:

1) Collect evidences by conducting systematic literature review.
2) Analyze the data.
3) Analyze the current payment landscape in Saudi Arabia.
4) Develop the proposed architectural framework.

2.2 Methodology:

The detail of each stage is described in the following sub-sections as well as in diagram 2.1.

2.2.1 Conducting Systematic literature review:
A detailed systematic literature review is conducted in the field of mobile payments as part of Chapter 3. The systematic literature review identifies the current status of mobile payment implementations and adaptations around the world to get more information with regard to the drivers and barriers of mobile payment adaptation. The research questions will be addressed and answered by the detailed systematic literature review as well as the proposed framework.

A review of the currently implemented solutions of mobile payments was discussed and the main successful implementations were covered in details in Chapter 4 to have more clarity regarding some of the globally-known initiatives in mobile payments.

Then, I will narrow the review to cover the local status of Saudi Arabia by conducting a complete study and analysis of the payment systems in the country as covered in Chapter 5 to understand how payment is being structured within the country and take advantage of some of the matured areas in payments to be integrated with the proposed mobile payment solution.

### 2.2.2 Analyze the data:

As a result of the literature review, a detailed data analysis will be carried to synthesis the gathered information and try to understand the main challenges surrounding mobile payment solutions in order to incorporate a solution for those challenges in the proposed framework. During the data gathering and analysis, a full understanding of the currently implemented technologies is expected to be achieved along with how those solutions can be adopted or modified to help in achieving our goal of a practical mobile payment solution for the Saudi market.

### 2.2.3 Analyze the current payment landscape in Saudi Arabia:

The Saudi payment landscape will be analyzed in details to understand the current capabilities and limitations and ensure reusing all possible exiting components.

### 2.2.4 Develop the proposed architectural framework:

A proposed framework will be discussed in Chapter 6 taking into consideration the result of the SLR as well other chapters covering the payments in Saudi Arabia and global implementations of mobile payments.
Diagram 2.1: Research Methodology

- Conduct Systematic Literature Review
- Collect and Analyse the Data
- Analyse the Current Payment Landscape in Saudi Arabia
- Develop an Architectural Framework
Chapter 3. Systematic Literature Review (SLR)
3.1 Introduction:

A systematic literature review (SLR) is a review which follows a predefined steps starting from the research question(s) [12], which makes it more focus and subject related. Systematic literature review is very helpful for new researchers or post-graduate students looking for proven and procedural steps to achieve an acceptable and scientific result.

There are many implementations or understanding of the SLR and the required steps to achieve it based on the research domain and area of interest. However, in this research I have followed the steps clearly described under the published “Guidelines for Performing Systematic Literature Reviews in Software Engineering” [10].

An example of such implementation can be found in [13] where the authors have conducted a systematic literature review to identify and classify tools that can be used in automating SLR process mainly in the software engineering domain. In this paper, the main research questions have focused mainly on identifying the tools and the stages where these tools can be used, search resources and key search strings to be used. Following this definition of the main approach, the authors have defined the inclusion and exclusion criteria to be applied against the identified papers. Finally and before presenting the result of the SLR, the authors have listed the data that will be extracted from each paper and synthesized at the end of the SLR process.

In [13], the authors have followed the SLR methodology to study software process improvement. As a starting point the authors have developed a protocol where search strings were defined and applied in different search engines where targeted papers are most likely found. A group of papers were identified based on the abstract and then thoroughly reviewed to identify the required papers for data extraction. The authors have pre-defined the expected type of data to be extracted which will help in achieving the answers of their main research questions.

Another example that used SLR to explore the best practices for successful design and implementation of software process assessment methods can be found in [14]. The authors have applied the SLR guidelines depicted in [10].

It is also worth mentioning that as per [10], there are two different reviews that complement SLR however they are not mandatory to conduct a complete SLR, those are:

1) Systematic Mapping Studies (aka Scoping Studies): this kind of study is usually required by a funding organization before they decide wither to proceed with the SLR in a specific subject or not.
2) Tertiary Reviews: is a systematic review of systematic reviews, which follows the same structure as the normal SLR however the reviewed papers are focused and includes only high quality of published SLR’.

The systematic literature review helps in identifying the best evidences published in the literature that are related to a certain topic in software engineering. This field of study is commonly known as Evidence-based Software Engineering (EBSE). EBSE is usually targeting taking decision regarding software development by combining up-to-date best evidences from research with practical experience [11]. EBSE doesn’t enforce one-for-all solution; instead it promotes the most suitable and expected to succeed solution based on the situation and circumstances of the environment where the suggested solution will be implemented [11].

In the case of EBSE, the software engineering shouldn’t depend mainly on lab results and it should encourage gathering evidences from real-life projects, observations and surveys [11]. Therefore, EBSE is integrated within this SLR to achieve the main steps listed below and suggested by [11]:

- Convert the problem into a question.
- Search for the best evidence.
- Assess and evaluate the evidence to ensure its validity and applicability.
- Integrate the identified evidences with the practical experience and customer’s expectations along with the circumstances in order to take the right decision.
- Evaluate the final solution and provide improvement suggestions.

3.2 SLR Process:

The process of conducting systematic literature review consists of three phases depending on each other. Each phase involves mandatory and optional steps with expected results or outcome of each step. However, in order to understand these phases, we need to understand the reasons for considering a systematic literature review which can be summarized in three main reasons [10]:

1) Summarizing the evidences related to specific technology.
2) Identifying gaps in specific research in order to propose new areas to be discussed.
3) Providing background in order to prepare for a new research.

Considering the above reasons, the SLR can be conducted by staring with the first phase which is planning the review this phase helps in preparing the review by understanding the need of the review and identifying the main research questions that will be discussed. As a result of this phase, a review protocol will be produced to be used as a main guideline for the research.
The second phase can be considered as the actual review or **conducting the review** which involves identifying all the candidate research papers and filtering them into primary papers. As a result of that the required data will be extracted from all those papers and further analyzed and synthesized in order to answer the main research questions.

Finally the result of the research will be documented in the third phase which covers the **reporting of the review** in a well-documented and formatted report which will be reviewed by higher authorities. A summary of these steps is provided in (Figure 3.1).
SLR Process (in nutshell):

**Phase 1: Planning the Review**
- Step 1: Identification of the need for a review
- Step 2: Specifying the research question(s)
- Step 3: Developing a review protocol

**Phase 2: Conducting the Review**
- Step 1: Identification of research
- Step 2: Selection of primary studies
- Step 3: Study quality assessment
- Step 4: Data extraction and monitoring
- Step 5: Data synthesis

**Phase 3: Reporting the Review**
- Step 1: Specifying dissemination mechanism
- Step 2: Formatting the main report

*Figure 3.1: SLR Process in Nutshell*
3.3 SLR for Mobile Payment

3.3.1 Planning the Review

i. The need for a review:

As the subject of mobile payment in Saudi Arabia is still immature and not yet implemented neither national-wide nor in a closed segment environment. It is necessary to conduct a review of the currently published information to understand the current status of mobile payment globally and use that as a benchmark and baseline for this study to formalize a practical mobile payment framework in Saudi Arabia.

ii. Research Questions:

The research questions that have been specified previously in section 2.1 are the following:

RQ1: How mobile can be used to make payment?

RQ2: What different approaches are there to make a successful mobile payment and how they differ?

RQ3: Are there any regulations in Saudi Arabia that regulate the mobile payment? If not, what suggestions and recommendations can be provided to set such regulations?

RQ4: Which mobile payment implementation framework is suitable for Saudi Arabia?

iii. Review Protocol:

The review protocol is defined to specify the methods that will be used to undertake the SLR [10]. Defining a protocol is important to avoid favoring or bias. The protocol usually contains all the required elements of the research in addition to planning information that will be used to govern the research activity.

A protocol will cover mainly the following points: identification of the research, selection of primary studies, study quality assessment, data extraction and synthesis as detailed below.
a. Identification of Research:

In order to identify the primary studies related to the research questions and in order to avoid a bias search strategy, the following search strategy was discussed and agreed with the supervisor:

- The following scientific resources were included in this review: IEEE Xplore, ACM Digital Library, and Google Scholar.

- Key word combinations differed from one resource to another based on the syntax of the targeted library.

- Title and abstract were used as the initial filtering mechanism while reviewing the papers.

- Only English-written and Arabic (if any) papers were included in this research.

- The result of “Mobile Payment” search term gave almost 11,100 results in Google Scholar therefore and due to the large number of results, it was decided to narrow the search in this source and make it more specific by including the “technology” term into the search keyword which gave reasonable number of results as shown in table 3.1.

<table>
<thead>
<tr>
<th>Source</th>
<th>Keyword</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Xplore</td>
<td>“Mobile payment”</td>
<td>243</td>
</tr>
<tr>
<td></td>
<td>“mobile payment framework”</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>“mobile payment factors”</td>
<td>0</td>
</tr>
<tr>
<td>Google Scholar</td>
<td>“Mobile + payment + technology”</td>
<td>329</td>
</tr>
<tr>
<td></td>
<td>“Mobile + payment + factors”</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>“Mobile + payment + framework”</td>
<td>122</td>
</tr>
<tr>
<td>ACM Digital Library</td>
<td>“Mobile payment”</td>
<td>246</td>
</tr>
<tr>
<td></td>
<td>“Mobile payment” “factors”</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>“Mobile payment framework”</td>
<td>5</td>
</tr>
</tbody>
</table>

*Table 3.1: Main search strings*
b. Selection of Primary Studies:
   Inclusion criteria:
   
   - Any research paper or study that explains the usage of mobile phones in payments.
   - Any research that describes the current mobile payment implementations globally.
   - Any research that compare different mobile payment implementations and the advantages and disadvantages of each implementation.
   - Any paper that describes an end to end mobile payment implementation with clear framework.
   - Any research paper that discuss the environment of mobile payment.

   Exclusion criteria:
   
   - Any study of mobile banking.
   - Any non-English/non-Arabic research where translation won’t be possible.
   - Any commercially-influenced research where the result is directed toward a specific product.

c. Study Quality Assessment:

   As suggested by the SLR guidelines [10], the SLR conducted by postgraduate students in their master or PhD work is revised by their supervisor to ensure that the protocol has been applied correctly. Hence, all selected studies will be reviewed by the supervisor for further analysis and approval.

   In addition to the review of the selected papers by the expert (supervisor), I have applied the checklist used by [15] to assess the quality of the selected papers, where a set of questions will be applied against each and every paper in systematic process to avoid bias and pre-judgment.

d. Data Extraction and Monitoring:
   The data extracted from each paper include the following:

   - The paper title.
   - The source (i.e. the conference or journal).
   - The year when the paper was published.
   - Classification of paper
   - Scope (Research trends or specific research question).
   - Summary of paper.
3.3.2 Conducting the Review

As a result of the detailed review of the identified papers, a subset of those papers consists of 43 papers were selected as the main papers to be studied in order to answer mainly the first two research questions RQ1 & RQ2. The reviewed papers were divided into 2 different groups to help in extracting the required data similar to the approach followed by the previously presented papers. The two groups are:

1. The main success factors.
2. Technology and solutions.

The aim of the review is to identify and understand how can we use the mobile phones in conducting payments, identifying the main stakeholders and players in the mobile payment domain, understanding the main factors that could affect the implementation and adaptation of mobile payment and finally identify different solutions proposed globally and the technology used in each one of them.

16 papers were grouped under the papers discussing success and failure factors while 27 papers were found to be discussing the implementation and solution of mobile payment, hence are related to the second group.

Those papers were assessed based on the checklist in [15] which consists of 10 questions used to evaluate the selected papers against scientific questions that help in assessing the overall process of paper selection. As a result of this assessment the below table 3.2 was developed which marks each paper against relevant question.

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
<th>No. of Papers (out of 43)</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is there a clear statement of the aims of the study? Yes/No. Score as 1, 0.5, 0.</td>
<td>43</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Is there an adequate description of the context in which the research or observation was carried out? Yes/Partly/No. Score as 1, 0.5, 0.</td>
<td>43</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>Was the research method appropriate to address the aims of the research? Yes/Partly/No/Not applicable (i.e. Expert Opinion). Score as 1, 0.5, 0 or mark NA.</td>
<td>27</td>
<td>62.79</td>
</tr>
<tr>
<td>4</td>
<td>Was the recruitment strategy (for human-based experiments and quasi-experiments) or experimental material or context (for lessons learnt) appropriate to the aims of the research? Yes/Partly/No/Not applicable (i.e. Expert Opinion). Score as 1, 0.5, 0 or mark NA.</td>
<td>35</td>
<td>81.39</td>
</tr>
<tr>
<td>5</td>
<td>Has the relationship between researcher and participants been considered to an adequate degree? Yes/Partly/No. Score as 1, 0.5, 0.</td>
<td>39</td>
<td>90.69</td>
</tr>
<tr>
<td>6</td>
<td>Is there a clear statement of findings? Yes/Partly/No. Score as 1, 0.5, 0.</td>
<td>43</td>
<td>100</td>
</tr>
<tr>
<td>7</td>
<td>Is the study of value for research or practice? Yes/Partly/No. Score as 1, 0.5, 0.</td>
<td>42</td>
<td>97.67</td>
</tr>
</tbody>
</table>

Table 3.2: Quality Assessment

Note: questions 5, 6 and 7 are having a low score due to the fact that those questions are applicable to empirical studies only.
Following the quality assessment of the papers, the following section will present the results of the data analysis conducted to extract the following information:

- Main success factors affecting the adoption and usage of mobile payment solutions globally.
- The most adopted mobile payment solutions based on different implementations in different countries.

### 3.4 Data Synthesis:

Taking into consideration the above mentioned technologies and solutions to implement mobile payment, it is very essential to ensure that the solution is adopted based on the capability of addressing the main success factors as covered by papers such as [3], [4], [6], [7], [16], [17], [18], and [19] which are summarized and ranked based on the frequency of discussed challenges in the reviewed papers in the below table 3.3 and figure 3.2:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Success Factor</th>
<th>Paper Reference #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security</td>
<td>[7],[20],[3],[16],[18],[19],[21],[22],[23]</td>
</tr>
<tr>
<td>2</td>
<td>Performance</td>
<td>[7],[3],[17],[21],[22],[24],[23]</td>
</tr>
<tr>
<td>3</td>
<td>Interoperability</td>
<td>[7],[3],[21],[22],[25],[23]</td>
</tr>
<tr>
<td>3</td>
<td>Cost effective</td>
<td>[3],[17],[19],[21],[22],[23]</td>
</tr>
<tr>
<td>4</td>
<td>Simplicity</td>
<td>[7],[3],[21],[25],[23]</td>
</tr>
<tr>
<td>4</td>
<td>Acceptance</td>
<td>[3],[4],[19],[21],[24]</td>
</tr>
<tr>
<td>5</td>
<td>Usability</td>
<td>[3],[19],[21],[24]</td>
</tr>
<tr>
<td>6</td>
<td>Efficiency</td>
<td>[7]</td>
</tr>
</tbody>
</table>

*Table 3.3: Success factors in implementing mobile payment solutions*

These factors are considered the drivers for any solution to address mobile payments. Hence, it is necessary to study each factor in more details to understand its effect on the mobile payment systems.
Figure 3.2: Percentage of Mobile Payment Success Factors discussed in the selected papers.

3.4.1 Security/Privacy:

Security is considered to be main concern that is applicable to all countries [7]. Therefore, security has been identified as a main success factor in electronic payment in general and mobile payment in particular [7].

In mobile payment, the following security issues and fraudulent attacks are always considered while addressing the security and privacy challenge, an example of those attacks can be summarized in the following issues: skimming, double spending and merchant fraud [26].

Various solutions that tackle the security issue have been depicted in the literature, for instance,

A biometric-based mobile payment was proposed by [27] to overcome the security concerns. The solution assumes that the customer will use an NFC-enabled mobile phone and in the same time all participating merchants are having NFC-equipped POS devices. The steps of the transactions are explained in figure 3.3 with the following steps:

1. Client approaches the cashier equipped with NFC-enabled POS and send the already scanned items in his mobile to the POS via NFC channel along with the value of customer ID, value N and value T which represents the uniqueness and time of transaction respectively.
2. Merchant using the POS scans the items in the shopping cart, decrypt the value received from step 1 using his private key and then generates a new value consists of merchant’s certificate.

3. Customer decrypts the value received in step 2 and validates the decrypted certificate. Once the result is satisfactory, the customer generates a new value signed by his certificate and sends it to the merchant. The message contains the fingerprint template (FPT) generated during the registration process.

4. Merchant decrypts the value received from step 3 and generate a new value based on the extracted data to be sent to the acquirer bank.

5. Acquirer decrypts the message and validate if the values generated by each party (i.e. customer and merchant) are matching such as transaction ID, transaction amount and time stamp. If all checks are successful then the acquirer generates a new message and sends it to the payment gateway.

6. The payment gateway will receive the message from the acquirer and perform the same validations performed in step 5. Then keeps a copy of the message and generates a new message to be sent to the issuer for authorization approval.

7. Issuer receives the new message from the payment gateway. Issuer bank will perform the necessary validations including the decryption of the value that contains the FPT, checks the client account for available balance, check of the received FPT matches the one stored at the issuer side, replicate the same checks performed by acquirer and payment gateway to ensure authenticity of the transaction. If all checks are successful then the transaction will be authorized as shown in steps 7 to 10 while the customer will be informed for security purpose directly in his mobile as represented by step 8.

![Figure 3.3: 2D-barcode solution to overcome the security issue [3]](image-url)
While this solution provides the required level of security, however the payment process is noticeably longer than the normal payment process using plastic cards. Also, dependency on multiple checks increases the false positive errors that might affect the successful rate of the transaction especially that finger prints captured at the merchant side might be slightly different than the ones that were captured during the registration due to the different devices used in both scenarios. Also, the performance of the system and transaction time needs to be measured to evaluate the customer experience and the required time for end to end on-site purchase.

Another solution to address the security concern was suggested by [28] as a cloud-based payment operational model. In this solution, the authors are proposing a payment model based on QR-codes (Quick Response Codes) where the customer has to be connected to the bank server to initiate the transaction as described in the below payments steps:

1. While paying at the cashier, the customer will launch the mobile app in his/her mobile and enters the preconfigured user and password.
2. The app will communicate with the bank server to confirm the enrollment of the customer in this service.
3. Once the availability of the service is confirmed, the bank server will initiate the QR code certificate service and sends a message with essential data to the mobile application.
4. Mobile App will use the received data and generate a QR code.
5. The cashier will scan the QR code displayed at the customer’s mobile phone.
6. The merchant system will decode the QR code and confirms the payment.

![Figure 3.4: A cloud-based with QR-codes solution to address the security issue](image)

In the solution as shown in figure 3.4, the researchers are claiming that having the bank server confirms and initiate the transaction at the beginning will help in ensuring genuine transactions data get processed. The solution is securing the end to end transaction lifecycle by securing the access to the bank server, the process of authorization Application in the mobile and the QR encoding and decoding process.
• Authorization Program (mobile App):

The mobile App is used as an interface to the bank server, where the customer needs to enter an account login details and then the server will verify and confirm the eligibility of this account to use the service, this approach will ensure the involvement of a centralized service managed by the bank which will strengthen the security of the authentication process. Also, the ability of the customer to limit the service to a specific merchant location or duration will help to reject any transaction initiated in different location or outside the approved durations.

• QR Code encoder/decoder:

The encoder is implemented in the mobile App while the decoder is available at the cash register for the merchant to complete the transaction. The mobile App will call the encoder after receiving the required data from the server to generate the QR code and the decoder will be launched by the register after scanning the QR code. The data that get encoded into the QR includes the international mobile equipment identity number (IMEI) which is a unique number for each handset similar to the MAC address of a computer, time and customer data. Those data are being encrypted and then used for the encoding process.

While this solution addresses most of the security concerns highlighted earlier, however it requires an online connection between the customer handset and the bank server which will eliminate any chance of having an offline authorization at the merchant side to accelerate the process which is usually an advantage of any mobile payment solution. However, this disadvantage could be eliminated by allowing a considerable amount of time for the QR certificate validity so the customer can generate the certificate before getting into the merchant and having it ready at the mobile app for the QR generation process.

3.4.2 Performance:

Performance expectancy is a main driver of customer acceptance and successful mobile payment implementation [17].

Performance was main evaluation criteria of the acceptance of the proposed mobile payment solution in [5] where the average transaction time was calculated over different network types such as EDGE, 3G, Bluetooth, WLAN, Fast Ethernet and NFC. The result shows low average time for NFC transaction for local transaction type (i.e. within the store).

The evaluation conducted by [5] shows that although an NFC-based transaction time is lower than others; however the decision of which technology will go with should be influenced by the environment and infrastructure capability where the solution will be deployed.
Balancing of performance and security is a real challenge [5][17], however this challenge should not impact the continuous efforts to ensure high performance of the suggested solution as the customer experience is disproportionate to the slow transaction time.

3.4.3 Interoperability:

In order for any mobile payment solution to be accepted and widely used, the support of interoperability is required [21]. Interoperability in mobile payment requires the support of any mobile phone or at least a good number of widely used brands in addition to the support of multiple cards/accounts from different participating banks.

Such requirement can be achieved based on the previously analyzed data by avoiding the hosting of the secure element (SE) in case of NFC solution as an embedded element within the handset which will restrict the customer from replacing the mobile without going through the process of registration again. Another consideration would be having a solution that can be linked to more than one account number as suggested by [21]. In this solution, the customer will be using the mobile number as the reference number which can be linked during the registration to one or many account numbers and getting stored in a centralized database that is used to lookup the required account number to perform the transaction based on customer preference. In this solution, the researchers have eliminated the issue of having only one account number registered for each customer as well as avoided the dependency on the handset itself which gives the solution the required interoperability and customer freedom.

This solution works as following:

- Every bank will be assigned a unique number which is called Bank ID.
- Multiple accounts for the same customer can be linked to one mobile number with the introduction of a Mobile Account Selector (MAS) value which will be used to identify the preferred account for payment.
- The payment is completed as shown in figure 3.5 (1) by entering the following values: mobile number, MAS, and transaction amount.
- Authentication will be performed with the issuer bank (2) and then a request will be initiated to the centralized database to lookup the required account number (3).
- The transaction will be routed then to the beneficiary’s bank based on the identified value from the centralized database (4).
- Steps from 5 to 8 shows the actual processing of the transaction, the confirmation to the customer’s bank and notification to the customer via SMS.
While in this solution the interoperability issue was eliminated by introducing a centralized database and a unique identifier for each account, however considering the expected number of customers using such solution, optimizing the database search function will be essential to avoid having huge impact on performance.

It is very clear by now that the key of the interoperability is avoiding dependency on phone manufacturers, mobile network operators or specific issuer bank. Therefore, for any solution to be interoperable, a centralized processor or database of customers will be always required. Such implementation was proposed by [26] and [28] which were presented previously in figures 3.3 and 3.4 respectively. In those solutions, the dependency was on the common features of any mobile phone to avoid restrictions; however those solutions introduce another type of challenges to the implementation team more than the customer. Those challenges are mainly the following:

- Online connectivity with the either the centralized database or the issuer bank.
- New equipment to be implemented by the merchants such as barcode readers.

The above analysis shows that implementing an interoperable solution is a challenging mission where designers are usually looking at interoperability from customer’s perspective only which is an important factor however they sometimes overlook the importance of having a solution that will not cost the merchants a considerable amount of money to replace their terminals or introduce new type of terminals.
3.4.4 Simplicity/Usability:

Simplicity and usability are usually linked to each other while building any solution. They are more concerned about the customer’s experience and how easy using the solution from customer’s perspective.

In general, payments require less number of steps and mobile payment is no different than other types of payments. Actually, in mobile payment the solution needs to be even simpler than using a plastic card in order to attract customers and convince them to use it. Therefore, our benchmark of the simplicity should be a comparison with the current payment methods and ensure that the proposed solution is at least in the same level of ease of use if not easier.

Going with the above understanding, it is clear that the solution will be simpler and easy to use if it doesn’t include connecting to a centralized server to retrieve data or generate barcode as suggested by [28]. The customer needs to feel that he/she doesn’t require connecting to the bank server or any other server to get more authenticity which will give wrong impression that the mobile itself is not a complete replacement of the plastic card.

In most of the NFC-based solution, the customer doesn’t need extra steps more than what he/she used to follow while paying by traditional plastic cards, which gives the customer the simplicity feeling considering that same steps are followed with no extra tools other than the mobile phone itself [3][27][29].

3.4.5 Cost Effectiveness:

Cost analysis while proposing any solution is a necessity. In the previously proposed mobile payment solutions, the financial impact on all participants in the payment chain, mainly customers and merchants is obvious. While various solutions are introducing secure setup [26][28], they mandate changes to the merchant’s equipment to cater for barcode scanners which might not be always acceptable by merchants due to the involved cost. Most of the solutions claim implementing a no setup cost mobile payment solution from customer’s perspective only which is part of the payment landscape but not the only part of it. Hence, a solution needs to ensure strong participation from merchants whom are the driver of such initiative by ensuring minimum investment from their side.

3.4.6 Acceptance:

Acceptance of mobile payment needs to be guaranteed from all payment stakeholders including customers, merchants, and issuer banks and in some cases mobile network operators.
In order to ensure adoption of their mobile payment solution, Japan has standardized the technology to be used by introducing Sony’s invented solution called FeliCa as a standard [4].

Standardizing the mobile payment implementation by a dominant stakeholder or a governance body will accelerate the adoption of the system by all participants including the customer who will see a consistent experience across all providers.

In addition to the standard regulations and implementations, merchants as a main stakeholder in the payment lifecycle will be attracted by a solution that gets easily integrated with their existing infrastructure and processes. The changes to the infrastructure can be perceived negatively as in the case of 2D-barcode solutions [26][28] while NFC-based solutions are usually welcomed by the merchants [30], especially in countries where contactless POS’s are already implemented which will make it easier for merchant to accept mobile payment.

Having the merchants accepts the implementation of mobile payment will increase the acceptance of the new payment method geographically which will influence the customers’ usage of the service.

After understanding the challenges needed to be addressed in any solution for mobile payment, it is essential to categorize those solutions into different technologies for actual payment during the mobile payment process suggested by the papers discussed in this SLR. Those technologies are ranked based on the frequency of suggesting them in different implementations as shown in figure 3.6.

It is also important to highlight that while NFC-based solution is widely used, however it was noticed during the review that many recent solutions are based on hybrid-technologies which
means combining NFC for actual payments at the merchant along with another technology for authentication such as 2D-barcode or biometrics. Therefore, it is important to highlight the different technologies used in those solutions from authentication perspective as well.

Another important aspect where different technologies were adopted is the authentication process. Authentication of customer is not necessary following similar technology as the actual payment technology, therefore the main technologies used for authentication are listed in the below figure 3.7 which shows different authentication preference including customer authentication based on mobile number via SMS/USSD, Web-based authentication using pre-configured credentials, Biometrics, or PIN-based authentication depending on the secured data stored in the phone (SIM-card, SD-card, embedded secure element, or cloud-based secure element).

![Solutions for authentication in Mobile Payment systems](image)

*Figure 3.7: Technologies used during authentication in mobile payment systems.*

It is worth highlighting that most of the reviewed papers were found to be published in China or by Chinese academic researchers. Figure 3.8 shows the country where the referenced paper was published while figure 3.9 shows the research sources with high percentage of researches obtained from IEEE.
3.5 Mobile payment solutions (based on the SLR):

Based on the SLR result, we can summarize the identified approaches to implement mobile payment solution as following:

- Near Field Communication (NFC-micro SD) technology
- NFC with Secure element in the SIM
- Biometric-based mobile payment
- 2D-Barcode
- Mobile payment in the cloud
In order to understand how each one of the above mentioned technologies can be used to implement mobile payment, we will need first to mention that mobile payment consists of two main phases which involves the usage of different technologies [31], the two stages are:

1) Personalization of the card data.
2) Authentication and transaction.

In the personalization of the card data, the customer information needed to conduct the payment will be generated and personalized in different ways. The customer data is stored in the secure element (SE); however the question will be where to store the SE itself. Based on the SLR analysis, there are multiple solutions for that as listed below:

a) Cloud-based SE.
b) Micro SD-based SE.
c) Handset-based SE.
d) SIM-based SE.

In this phase we can group the solutions into two different groups, one group considers using the phone itself or its main components and the other group uses the cloud to store the data.

In the other hand authentication and transaction phase can be implemented using one of the below technologies:

a) Near-field communication technology (NFC).
b) Biometric-based authentication.
c) Barcodes.

Therefore, mobile payment solution will be based on the combination of both groups. In order to have more understanding with regard to these solutions, I will discuss in details how each proposed solution work.

3.5.1 NFC-based Solution:

In any solution targeting to implement mobile payment using NFC technology, the following implementations needs to be arranged [32]:

- NFC Chip: which enables the phone to send the required data to the reader at the merchant side such NFC-enabled POS.
- Mobile App: the solution clearly needs to have a mobile app to act as an interface between the customer and the service provider(s).
- Secure element (SE): which is nothing more than a smart card module similar to the SIM card used in the telecommunication field. The secure element is expected to store the customer data in a restricted area.
- Personalization of card/account information: similar to any credit or debit card personalization process where the customer’s account information get personalized into the magnetic stripe or the chip of the plastic card, similar information will personalized into the secure element of the mobile.

The critical role of personalizing the customer information into the mobile requires a trusted party that has access to both card data and secure element of the mobile, and that’s why the new role of trusted service manager (TSM) has been introduced in the mobile payment ecosystem [32].

The main function of the TSM is to manage and personalize the NFC applications securely. Also, the TSM will be connecting the both worlds of card issuers (banks) and telecommunication companies.

The main capabilities required for a TSM function [32]:

- Management of Mobile Network Operators (MNO).
- Over-The-Air (OTA) provisioning capabilities to personalize the secure element hosted in the mobile SIM remotely.
- Mobile application management.
- Management of the relationship with the banks/card issuers.

NFC-based mobile payment can be implemented as well by using the mobile phone components to store the SE and NFC technology to perform the payment. As an example of such implementation, the solution proposed in [3] where the customer information will be personalized in the micro SD card (memory card) by the issuer bank and then using NFC technology the customer can initiate and complete the payment transaction at the merchant store. The payment transaction flow proposed by this solution can be described in the following steps:

1. Customer chooses the application installed earlier in his/her mobile phone.
2. After entering the account number and password configured earlier by the customer during the registration process, he/she chooses the preferred card (credit or debit card for example) which has been stored in the SD card memory during the personalization process.
3. Then, the customer will put the mobile phone closer to the reader at the merchant store.
4. The encrypted information required to perform the transaction will be transmitted over NFC channel to the merchant device which will initiate normal payment transaction similar to the one initiated by a normal plastic card.
Considering the above details of the NFC-based mobile solution and the critical role of the secure element (SE) which consists of secure memory that can be embedded into the UICC (Universal Integrated Circuit Card) that is used by telecommunication companies to host the customer information or it can be embedded into the mobile device itself [31], we can classify the usage of mobiles in payments based on the location of the SE as following:

- Using the mobile phone components such as Mobile Network Operator SIM card, micro-SD card to embed the SE, or embedding the SE into the device itself (hardware of the mobile phone).

- Hosting the SE into the cloud and using the internet connectivity to access the data and initiate transactions.

- Using the mobile phone as an instrument/tool to initiate the payment either using Web technology or SMS however verification will be always completed by referring to the card issuer server and confirmation can be done using secure data such as data presented by barcodes.

- To give more clarity with regard using the mobile phones in conducting payments, we can consider the technique of hosting the SE in the mobile itself or in a component that is attached to the mobile phone such as the memory card (SD card) which will be communicating with other components of the mobile payment ecosystem via the NFC technology (Near-Field Communication) which will transmit the card data to the point-of-sale device at the merchant using the mobile phone to make payment. This technique is described in details by the below Figure 3.10 [3]:

![Figure 3.10: NFC-Micro SD Solution][3]

- In this scenario, (1) the information service provider or the technical team within the bank will develop the mobile application based on the requirement of the micro SD provider. On the hand, (3) the personalization company that is currently preparing the
bank card will follow the same procedure to personalize the micro SD after (2) getting the card information from the card issuer.

- Once the personalization of the data into the micro SD is completed, then the application developed by the card issuer is downloaded and installed into the customer’s mobile phone can be used to interact with the NFC-enabled point-of-sale at the merchant to initiate the payment transaction which will be communicated to the card issuer server for confirmation as explained in diagram 3.1.

- This scenario is an example of mobile phone acting exactly as the current payment plastic cards where instead of storing the customer data into the chip card embedded into the plastic card; the same data is stored into the mobile phone.

![Diagram 3.1: NFC Mobile Payment](image)

### 3.5.2 Biometric-based solution:

Biometric-based technology is used in mobile payment to authenticate the customer while using another technology such as NFC to conduct the actual payment.

In [27] based on hybrid-technology by implementing biometric and NFC technologies with the card data stored in the SIM which can be described by the following steps:

1. During the registration process, the client will launch the application in the mobile and keeps his/her finger on the finger print scanner.
2. Finger print scanner generates a captured finger print template (FPT) and sends it to the mobile biometric application (MBA).
3. Finger print template is stored in the mobile payment application for future transactions.
4. During the payment phase, multiple decryptions activities between customer device and POS device takes place and then once all checks are successful a new set of transactions initiated with the issuer for extra checks, once the validations are corrected then the transaction is confirmed to the customer and the merchant.

3.5.3 Barcode-based solution:

Another solution to be discussed is based on 2D-barcode as proposed in [26] where the researcher has suggested using barcode technology on mobile phones to be read or scanned by the POS at the merchant side to decrypt the secured information and complete the transaction. The process of the suggested solution works as below:

1. During registration, the customer must be physically present where he/she will provide the bank number and other information required to complete the transaction, subsequently the customer will receive an account number and shared key to complete the registration.

2. As the payment scheme in this solution is based on 2D-barcode and hash-chains. Every hash element has a value and can be used to pay at merchants only after registration where the customer will register the chain of hash values with the authorized broker or bank before spending. Once the confirmation which is received via SMS is completed then the customer can only spend from the committed chain.

3. During payment, the following scenario is experienced:

- Customer will prepare a package to pay which consists of customer id, a hash element and the sequence number of the element in the chain which is called a Payment Package (PP).
- After having the PP generated, customer will have to present it as a 2D-barcode.
- The merchant will scan the PP as presented in the customer’s mobile phone screen.
- The scanned PP is then sent to the authorized broker or bank for verification.
- After receiving the commitment which is presented in PP, the broker will debit the chain value from the customer account and the transaction is completed.

The payment model using 2D-barcode is described in the below figure 3.11:
3.5.4 Cloud-based solution:

A final solution that can be explored is the implementation of mobile payment using cloud computing, in [33] the researchers are proposing a cloud-based payment solution using NFC technology, the steps describing the proposed process is listed below:

1. Customer holds his phone in front of the reader to make payment.
2. The payment application is downloaded into the mobile SE.
3. The reader communicates with the cloud to confirm the customer balance.
4. Balance will be confirmed by the cloud.
5. Based on the provided information the transaction will be completed or rejected.
6. Reader will update the cloud with update the customer’s account balance.

![Diagram of payment model using 2D-barcode.](image)

*Figure 3.11: The payment model using 2D-barcode [26].*

*Figure 3.12: Proposed solution for cloud-based NFC payment system [33].*
The use of cloud computing in the mobile payment is usually depending on the use of another technology such as Quick response codes (QR-codes) which represents the two-dimensional barcodes to perform the actual payment. Such implementation is proposed in [28] as detailed in the below sequence diagram 3.2:

Based on the above presented solutions and payment methods using mobiles, we have answered the first two questions in the research:

**RQ1:** How mobile can be used to make payment?

**RQ2:** What different approaches are there to make a successful mobile payment and how they differ?
3.5.5 Solutions vs. Challenges:

In the below table 3.3, the challenges addressed by each proposed solution along with the difficulties expected during implementations as suggested by papers [3], [20], [26], [27], [28], [31], [34] and [35]:

<table>
<thead>
<tr>
<th>Proposed Technology/Solution</th>
<th>References</th>
<th>Advantages/Issues addressed</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| Mobile payment in the cloud (Secure element in the Cloud) | [12],[20], [28] | Platform-free with no restriction on mobile brand or OS. | • ID validation  
• Administration  
• Customer information |
| 2D-Barcode | [26] | • Simplicity  
• No setup cost for customers  
• Low processing cost  
• Overspending and merchant fraud prevention by using hash-chain | • Merchant setup cost (scanners and connections)  
• Online connection is required |
| NFC-micro SD | [3] | • Resolve the issue of the required collaboration in the value chain  
• In sync with the trend of replacing phones frequently by customers  
• Keep the main players in the payment chain with no changes and no dependency on a new player such as telecoms. | • Not all mobile phones support micro SD (iPhone as an example) |
| NFC with SE in the SIM | [30],[31] | • Security | • Dependency on telecoms |
| Biometric-based solution | [27], [34] | • Security.  
• Hard to be spoofed.  
• Cannot be shared or lost.  
• Unique to each user.  
• No need to remember a password or carry a token.  
• Biometric capability is already implemented in the main mobile phones and easy to be attached if required. | • Biometric template security, once a biometric is lost then it is lost forever and cannot be reset or replaced. |
| Mobile payment based on mobile phone number | [36] | • Suitable to access contents on the web.  
- Easy to register customers based on their mobile number.  
- No dependency on mobile phone devices. | • Security concerns.  
- Not suitable for the in-store purchases. |

Table 3.3: Proposed solutions, advantages and disadvantages

### 3.6 Conclusion:

To summarize the main design factors out of the challenges studied in the previous sections

- **Interoperability** is the key to have continuous usage of the service.
- **Interoperability** should be considered at all levels including mobile phones, issuer banks and in some times mobile network operators (MNO).
- **Usability** and **simplicity** of the system should be benchmarked against current process to avoid having more complicated process that can impact the customer experience of the new method.
- **Cost** of the service shouldn’t be charged to the customer; instead banks should consider this service with the initial setup cost as a saving of the current cost incurred for card production. Also, merchants should not be impacted by a massive change to the environment and infrastructure which might cost them more than the benefits and the value of the service.
- Having standard setup and rules for the mobile payment implementation will ensure **acceptance** by all stakeholders and consistence experience by customers.
- **Security** is always a concern and shouldn’t be ignored during the design of the system. However, it shouldn’t impact the final service provided which might impact customers’ acceptance.
- **Performance** of the system is a debatable factor due to the impact of the existing infrastructure of the targeted environment. Hence, a limited implementation of the service for a specific type of transactions might help in controlling the level of the provided performance.

As shown in figure 3.13, mobile payment solution is designed based on the overlapping of three important factors, those are: virtual card storage which carries the customer account data similar to the actual plastic card, authentication, and actual payment the replaces the swipe or insert of the plastic card into the point-of-sale machine.
.7 SLR Validity Threats:

We faced many challenges during the SLR to ensure the validity of the final result. These challenges or threats are listed below with the actions taken to mitigate their impact.

- Selecting primary studies:

Selecting the primary studies for the SLR was a major challenge with the threat of the possibility in missing some publications or overlooking proven study. Therefore, the selection has been conducted in multiple iterations to ensure the same result is retrieved for each search term every time from each research source included in the study.

- Selection and extraction of data:

The analysis of the selected studies is an important phase of the SLR, hence, it has been agreed to re-evaluate the extracted data by the supervisor to confirm the full coverage of the available data from the selected sources.

- Missing some success factors

Success factors of mobile payment implementations is a major outcome from the conducted SLR, and the threat of missing some of those factors was identified and addressed by repeating the exercise multiple times and evaluating the extracted data and identified factors.
Chapter 4. Real-life examples of Mobile Payment Implementations
4.1 Introduction:

There are many successful implementations of mobile payments worldwide with different approaches and technologies depending on the objective, environment and customer needs.

Some of the globally recognized mobile payment solutions in the market are listed below:

- Starbucks Mobile Payment in United States.
- Google Wallet.
- LoopPay Wallet.
- Softcard (previously known as ISIS) in the United States.
- Apple Pay.

In the below sections, I will be describing the details of those mobile payment solutions:

4.2 Starbucks Mobile Payment Solution:

Using Starbucks mobile application, a customer can pay for his/her coffee at any Starbucks stores participating in this service.

Starbucks implementation depends mainly on a 2D-barcode that gets displayed on the screen by using the downloadable mobile app and loading the prepaid card details into the application.

The customer will need to configure a prepaid Starbucks card into the application and follow the below steps:

1. Once the prepaid card is configure in the wallet you can select the card and touch the “Touch to Pay” sign as shown below.

2. You can also reload the Starbuck prepaid card by configuring your credit card information into the application which will allow recharging/reloading the prepaid card whenever required.
Starbucks app allows customers to use only the prepaid card provided by the largest coffee chain instead of enabling mobile payment for all of your payments which means you only replace the wallet for Starbucks purchases for now.

### 4.3 Google Wallet:

Google wallet is an Android-based application that uses the embedded secure element (SE) in the NFC-enabled mobile phone that is compatible with this wallet to facilitate mobile payment via NFC technology.
Therefore, the solution is considered to be built based on the following technologies:

- Card data is personalized in an embedded secure-element within the mobile handset.
- NFC technology is used to transmit the data between the mobile wallet and devices at merchants.

Below diagram 4.3 illustrates the steps of Google Wallet transaction:

1. The app requests card information from the wallet via secure channel.
2. Google wallet responds with the required information.
3. In this step, the App requests for a full access to the google wallet.
4. Google wallet responds with full information which contains the credit card details as well.
5. The app confirms back to google wallet the status of the transaction (approved/declined) after completing the required steps with the payment processor.

![Diagram 4.3: google wallet transaction (Google.com)](image)

**4.4 LoopPay Wallet:**

In LoopPay wallet, the customer can purchase the LoopPay Fob and LoopPay ChargeCase (diagram 4.4) which are required to complete the setup and the transaction as described below.
1. After receiving the LoopPay Fob or LoopPay ChargeCase, the customer can swipe all his/her cards using the Fob connected to the iPhone and then the card information will be stored into the wallet for future use.
2. A PIN will be also configured as part of the setup process.
3. During the transaction, the customer will chose one of the already configured cards in the wallet and using the ChargeCase which is NFC-enabled the customer can initiate the transaction at any contactless-enabled POS in the market.
4. LoopPay wallet differentiates itself by not depending on any card issuer or mobile network operator to empower the mobile for payments.

4.5 Softcard:

Softcard mobile wallet (or previously known as ISIS) is a joint-venture company established by the largest mobile network operators in USA. Softcard supports most of the bank issuers in the US and follows easy steps to setup a card and use it at the participating merchant stores.

The main steps describing the setup of a new card us listed below:

1. Get a compatible android-based phone with NFC or an iPhone case equipped with NFC capability.
2. Get an enhanced SIM card from your mobile network provider which contains a secure element (SE).
3. Download Softcard application from the online store.
4. Setup a new user id and a 4-digit PIN that will be used during the transaction time.
5. To add a card to your newly installed app, you open the application and select the preconfigured cards or select to setup a new type of cards with a participating issuer.

6. The setup will need to be completed at the issuer bank website as shown below.

7. After installing your card into the app, you can easily select the required card during the transaction time and tap your mobile phone into the merchant device supporting the NFC transaction which will trigger the required information to be transferred via the NFC connection to the merchant terminal and then follow the normal transaction flow similar to a normal plastic card.
4.6 Apple Pay:

Apple Pay is the new joiner to the mobile payment arena, where Apple has officially launched its payment solution in October 2014. The following features are the main characteristics of this new solution:

- NFC-based transactions.
- Using biometrics for authentication by leveraging iPhone new feature which is called Touch ID.
- It doesn’t store any sensitive card data in the mobile; instead it uses the new “Tokenization” concept to replace the sensitive data with dummy numbers.
- It is only supported by latest iPhone models and Apple products such as Apple Watch.

4.7 Google Wallet vs. Apple Pay:

The below table 4.1 compares google wallet vs. apple pay as the two main globally identified competitors when it comes to mobile payment initiatives:

<table>
<thead>
<tr>
<th></th>
<th>Apple Pay</th>
<th>Google Wallet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payment technology</strong></td>
<td>NFC</td>
<td>NFC</td>
</tr>
<tr>
<td><strong>Authentication method</strong></td>
<td>Biometric (fingerprint)</td>
<td>PIN</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Use Tokenization</td>
<td>Use virtual card</td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td>Apple products only</td>
<td>All</td>
</tr>
</tbody>
</table>

*Table 4.1: Google Wallet vs. Apple Pay*
Chapter 5. Payments in Saudi Arabia
5.1 Introduction:

Saudi Arabian Monetary Agency (SAMA) – the central bank of Saudi Arabia - is controlling and managing all payment systems within the country with the support of the Saudi banks and other international banks operating locally [37].

The main components of the Saudi payment ecosystem includes: SARIE, SPAN, SADAD and cheque clearing systems.

In 1997, Saudi Arabian Riyal Interbank Express (SARIE) system was introduced which acts as the Real Time Gross Settlement system (RTGS). SARIE eliminate the need of having interbank settlement and gives more visibility and control over local transfers between Saudi banks. It is also used as the settlement backbone for all other payment systems operating locally [37].

Saudi Payment Network (SPAN) was introduced to support connecting all cross-bank ATM (1990) and POS (1993) transactions. The system is centralized in SAMA and connecting all issuer (card owners) and acquirer (device owners) banks to each other to facilitate the processing of transactions without the need of having direct connections between each two banks.

The electronic bill presentment and payment system (SADAD) is the newest joiner to the Saudi payment ecosystem which was officially implemented in 2007. SADAD provides a centralized system that connects all Saudi banks and billers to facilitate paying one-off and recurring bills [37].

As noticed in the previous paragraphs, the central bank in Saudi Arabia plays a significant role not only in regulating the payment market but also managing and operating in some of the cases the day-to-day activities within the Saudi payment market.

5.2 Cashless Payment:

Different systems within the Saudi ecosystem support different cashless transactions, the main cashless transactions are listed below [37]:

- **Credit Transfer**: SARIE system is used to transfer credit between banks for settlement purposes as well as performing customer-to-customer credit transfer. In addition to that, most of the public and private payrolls are being paid/credited via SARIE system.

- **Payment Cards**: SPAN cards issued by the locally-operated banks are used for ATM and POS transactions where customers can use their cards at any SPAN-enabled ATM or POS without the need to be charged for this service. The implementation of SPAN cards was upgraded to chip technology based on EMV standard in 2010 and all magnetic cards where replaced with chip cards by the end of 2012.
• **Prepaid debit cards**: prepaid cards are account-based cards supporting ATM and POS transactions. Those cards were mainly introduced to facilitate the participation of unbanked customers whom usually use cash only in their day-to-day transactions. Hence prepaid cards can be issued under one of the following category: Payroll, student, expense cards, and gift cards.

### 5.3 Payment Systems:

The main payment systems within Saudi Arabia can be summarized as: SARIE, SPAN and SADAD. Therefore, we will go into the details of each system operating model to help understanding how the payment ecosystem is locally operating.

#### 5.3.1 SARIE:

SARIE system is a core system and main component within payment infrastructure in Saudi Arabia. SARIE acts as the backbone of the fund transfer locally including the settlement of the other systems transactions such as SPAN and SADAD. SARIE system is located at SAMA’s head office and all banks are connected to the system via proprietary interface over SAMA joint network which is a private network for most of SAMA’s systems [37].

All participants to SARIE system are banks as per to SAMA regulations, however there is no requirement with regard to the number of transactions supported by each bank [37].

SARIE supports credit transfers as well as direct debits; the messages supported by SARIE are built based on SWIFT standards format. Both single and bulk transfers are supported by SARIE [37].

SARIE is operating only during working days from 9:00 to 16:00 hrs., this is considered to be a challenge for the customers by not offering a 24-hours operating model [37].

Technically, SARIE system supports many security features to ensure a controlled environment and secured transaction, those features include the following:

- Digital signature.
- Encrypted connections.
- Secure access to SARIE workstations.
5.3.2 SPAN:

The Saudi Payment Network which was introduced in 1990 for ATM transactions and started supporting POS in 1993 has grown rapidly in terms of number of devices and transactions [37]. SPAN currently is fully EMV-compliant network which increase the security of the transactions and encourage more usage of the network. Membership of SPAN is restricted to only financial institutions including issuers and acquirers. The member banks can be either issuer or issuer and acquirer in the same time. Merchants are participating in the SPAN system however they are not members [37].

5.3.2.1 Type of transactions:

SPAN acts as a switch to facilitate ATM transactions between banks with direct connections with all members of SPAN network to ensure consistency in supporting the main transaction types such as Cash Withdrawal, Balance Inquiry and Mini statement. However POS network is operating in slightly different approach where all POS’s in the market connected directly to SPAN switch and then SPAN will route the transaction accordingly to the issuer and acquirer banks. Banks-merchant relationship is still maintained by the acquirer banks and they still own the terminals based on agreement with the merchants [38].

All banks must be capable of supporting at least the following transactions [39]:

- POS Transactions:
  - Purchase.
  - Refund.
  - Reversal.

- ATM Transactions:
  - Cash Withdrawal.
  - Balance Inquiry.
  - Mini Statement.
  - Reversal.

5.3.2.2 Technical Design:

Figure 5.1 illustrates the connectivity and transaction flow for ATM transactions in the SPAN network [38].
5.3.3 SADAD:

SADAD network was launched by SAMA in 2004 to act as a centralized national electronic bill presentment and payment system where all local banks along with registered/enrolled billers are connected to facilitate paying one-time or recurring bills and invoices.
SADAD model can be illustrated by the below diagram 5.3:

![Diagram of SADAD model](www.sadad.com)

**Figure 5.3: SADAD model (www.sadad.com)**

5.3.3.1 **Type of transactions:**

SADAD supports the following type of transactions:

- **Online Payment**: this type of transactions requires an online connection with the targeted biller where the transaction gets initiated by the member bank and then SADAD will complete the other leg with the connected biller.

- **Offline Payment**: this type of transactions doesn't require the online interface between SADAD and participated biller, instead the biller will be uploading the bills in agreed frequency to SADAD server and then all connected banks can inquire the uploaded bill and facilitate payment online, however the confirmation from SADAD to the biller takes place in an offline fashion where SADAD delivers all payments to the biller server based on agreed forma and frequency.
5.4 Conclusion:

Based on the above reviewed designs and regulations as stated in [37]-[38]-[39]-[40], we can summarize the main rules that regulate the payment systems in Saudi Arabia in the following points:

- A licensed bank only is allowed to be connected to SPAN.
- The applicant bank will be certified for successful implementations in connectivity, transactions, and card issuance.
- All issued cards must be compliant with EMV standard.
- PIN security standards must be adhered to during the PIN selection and transaction.
- All acquirer banks must be issuers.
- Acquirers must ensure POS’s are compliant with security requirements related to PED.
- Banks must comply with the Payment Card Industry Standards (PCI-DSS).
- All POS’s are directly connected to SPAN switch.

Based on the above we can clearly answer RQ3 and state that mobile payment solution is not yet implemented in Saudi Arabia and hence there was no mention of the mobile payment in the presented ecosystem in the country. As a result, there are no mobile payment specific regulations or rules that can govern the implementation of such solution other than the overall payment regulations presented in earlier sections.

However, we can notice that SAMA’s role in the payment ecosystem is vital and cannot be ignored, which means that SAMA via its payment instruments (SPAN and SADAD) must be part of any proposed solution to implement mobile payment transactions in Saudi Arabia.

In order to confirm the status of mobile payment in Saudi Arabia, I have contacted the executive teams in SPAN and SADAD and interviewed them to get their point of view. The result of those interviews with the Head of System Development in SAMA focusing on the SPAN service and Head of IT Development in SADAD is summarized below:

1. **Is there a mobile payment solution live in Saudi Arabia?**
   No, as of today there is no mobile payment solution implemented or piloted in KSA.

2. **Is there a regulation prevent mobile payment implementations in Saudi Arabia?**
   There is no specific regulation that prevents mobile payments implementation in KSA, however SAMA is the entity responsible for regulating the Payment industry in Saudi Arabia, thus any payment solution has to be approving by SAMA.
3. **Do you have plans to implement mobile payment in the local market?**
Yes, there are plans to implement a nationwide mobile payments solution, recently there are exploration activities conducted to assess which technology is best fit for the local market, as new mobile payments technologies emerge the eco system keeps changing.

4. **How do you see the future of mobile payment in Saudi Arabia?**
With the young demographics of the Kingdom and with over 80% of retail payments volume currently executed in cash, the potential of mobile as an important payments channel is very high; however I do not foresee that mobile payments will replace cards rather than complementing it. Therefore banks and SAMA are working together to enable this service in the most suitable way to the local market.
Chapter 6. Architectural Framework for Mobile Payment Application in Saudi Market
6.1 Introduction:

As we have seen in chapter 3, researchers have identified the main factors affecting the implementation of mobile payments as well as the customer acceptance of the new service. Those factors along with the local drivers and regulations of payments in Saudi Arabia presented in chapter 5 should be considered while proposing a framework for mobile payment.

Therefore, the following factors are identified based on the global trends and drivers as well as the local regulations and limitations which will directly impact the design of any proposed mobile payment application framework that is expected to be integrated smoothly with the existing payment landscape and need to be satisfied to ensure successful implementation:

- **SPAN scheme as the national card scheme in Saudi Arabia:**
  Standardizing the mobile payment rules will build a baseline that will be easily adopted by all stakeholders similar to the Japan case presented earlier in the SLR.

- **High penetration rate of mobile subscribers in Saudi Arabia that reaches 170%** ([www.CITC.gov.sa](http://www.CITC.gov.sa)) will lead to adopting interoperable solution in terms of supported mobiles as well as supported issuer banks which also supports the interoperability factor highlighted in the SLR.

- **Support of multiple bank accounts/cards** to ensure customer’s continuity.

- **Adaptable to any new payment solution** by customers and merchants.

- **Security and privacy of data.**

The above highlighted factors will impact the design of the mobile payment application framework for the Saudi market and shouldn’t be ignored. Each one of these factors will derive a design component that satisfies relevant requirement. The proposed solution will leverage on the local market factors and on the previously presented solutions such as cloud-based mobile payment, NFC-based mobile payment and others.

6.2 ISO/IEC/IEEE 42010 Standard:

ISO 42010 standard which was developed for architectural description in systems and software engineering addresses the creation and analysis of the system and software architecture will be
used as a base for the proposed architectural framework to present the final solution in an abstract yet descriptive format.

The standard states that an architecture framework should include the following [41]:

1) Information to identify the architecture framework.
2) Stakeholders.
3) One or more concerns such as the purpose of the system/software, the suitability of the architecture for achieving the purpose, the feasibility of implementing the system/software and the maintainability and evolvability of the system/software.
4) Architecture viewpoints: where each concern identified in the architecture framework should be governed by at least one viewpoint to express the way we look into the system/software resulting in having one or more views.

Considering the above guidelines proposed by ISO 42010 standard, I will be applying the same into the proposed mobile payment architectural framework before presenting the final result of the framework in the following sections.

### 6.2.1 Stakeholders:

In this proposed solution, the main stakeholders are identified to be users of the system or the regular cardholders, merchants whom are accepting the payments at their stores, SAMA as the owner of the SPAN scheme and definitely the issuer banks owning the payment card.

### 6.2.2 Concerns:

Concerns are the area of interests for the identified stakeholders. Based on the previous section, we have four main stakeholders whom are interested in the system and expecting specific concerns to be addressed by the proposed architectural framework. Those concerns are mainly the success factors identified during the literature review where some of them are common concerns among all stakeholders others will be specifically addressing one stakeholder’s concern.

The main concerns associated with their respective stakeholders can be seen in the below table 6.1 which shows the traceability of each concern.
### 6.2.3 Architecture viewpoints:

Considering the fact that Interoperability concern is common among all stakeholders, I will be addressing this concern in the form of the following “operational” viewpoint described in figure 6.1 which describes the system in its live environment.

![Figure 6.1: Operational View for the interoperability concern](image)

The above figure 6.1 can be traced as following:

1. Customer will initiate the registration process in the mobile payment via any member bank.
2. The registered bank will initiate and complete the registration on behalf of the customer with SPAN.
3. SPAN will confirm back with the successful registration.
4. Notification will be sent to the customer instantly.
5. The customer, using any mobile phone will download the SPAN wallet from the respective store.
6. The installed wallet will communicate with SPAN and download the customer information to be personalized.

Following the above steps, the customer can use any bank account with any mobile phone at any certain point of time to enable his/her mobile to be fully equipped with the mobile payment capability.

The following sections will describe in details the proposed solution with detailed operational viewpoint covering all aspects of the solution.

6.3 Proposed solution:

Considering the factors in the previous sections, the proposed solution for the Saudi market should have the following characteristics:

- A Wallet-based mobile payment solution owned by SAMA as the SPAN Wallet which will provide the flexibility of adding and removing bank accounts/cards whenever is required based on customers’ preference and not to limit the mobile payment feature to specific bank account or specific mobile handset.
- SPAN Wallet will support all debit cards issued by any SPAN member bank.
- SPAN Wallet will be hosted and managed centrally by SAMA.
- The new Wallet will support NFC transaction which is supported by most of the currently installed POS in the market.
- SAMA will play the role of the Payment Manager by owning the wallet, the creation and management of payments.
- Customers will be able to enroll into the SPAN wallet service via their banks’ internet banking channels which will be directly connected to the centralized solution at SAMA.
- Customers can always re-download their SPAN Wallet from the centralized system using their ID, Wallet PIN that was configured during the initial enrollment and a one-time-password that will be sent to the configured mobile number.

The above characteristics of the proposed solution are the main functional requirements extracted by considering the success factors as well as the current payment ecosystem capabilities in Saudi Arabia; however NFRs (non-functional requirements) are main drivers of any software implementation and cannot be ignored while proposing this architectural framework. Therefore, I will be considering two out of the main success factors identified earlier and evaluate how the solution will address them. The selected factors are security and interoperability.
6.3.1 Security:

Security in payments is always a main factor and challenging requirement that cannot be ignored due to the criticality of the payment process. Payment cards are as good as actual cash in value due to the included information in each transaction such as card number, expiry date and card verification value which all together can be used to complete a successful transaction. In the other hand, trying to secure that information in the mobile device will require utilizing the secure element (SE) which will open the challenge of ownership of this SE as discussed earlier. In order to overcome this challenging requirement we will have to eliminate the use of critical card data, mainly the card number. To do so, tokenization as described in [42] can be a solution for this challenge which is considered in the proposed architectural framework. By implementing tokenization, a new role will be considered which can be assigned to an existing player in the payment ecosystem:

- **Token Service Provider:**

  In our case, SPAN using the SPAN Wallet Server will act as the token service provider assigning tokens to the requestor who is in this case will be the mobile wallet customer via his/her issuer bank.

Introducing tokenization will require mandating new fields to construct the payment message. The following fields will be the main mandatory fields in the new system:

- **Token Number:** This will replace the traditional Primary Account Number (PAN) issued by the card issuer bank.
- **Token Expiry Date.**
- **Token cryptogram:** this field will provide assurance to the Token Service Provider with regard to the token requestor. A public key-private key encryption can be used while provisioning the wallet by the SPAN Wallet Server.
- **Token PIN.**

By introducing token numbers, the risk of exposing card numbers (PAN) will be eliminated which will reduce the risk of fraudulent transactions as described later in this chapter. In order to complement the secure token number, the provided token by SPAN wallet server in our case will be encrypted by a PIN number generated during the registration of the customer where the same PIN has to be provided during payment.
6.3.2 Interoperability:

Interoperability of the proposed solution can be addressed from different perspectives, those are: customer, merchant and banks.

Customer:

- Possibility of using the mobile payment application in any mobile phone:
  
  The proposed application will have versions for iOS and Android mobiles to ensure covering customers’ needs.

- Dependency on mobile network operators (MNOs).
  
  The proposed solution will not have dependency on any mobile network provider which will give the customer a freedom to use any of his/her mobiles.

- Dependency on specific issuer bank.
  
  By centralizing the wallet holding the entire customer’s card information in SPAN server as well as integrating with all issuer banks via a standard interface, we will be eliminating the dependency on specific issuer bank(s), which will ensure the interoperability of the solution in terms of allowed cards.

Merchants:

Merchants will not need to change any of their equipment; instead an updated version of SPAN POS will be installed in all POS’s which will accept such payment instantly.

Banks:

- Interfacing requirement.
  
  Other than integrating with SPAN server for registration and enrollment, banks will not need to change their existing payment systems to cater for the mobile payment transactions; instead SPAN will initiate a normal card transaction to the issuer bank for approval whenever required. This design factor will help banks to participate into the solution with the minimum changes and ensure compatibility of the currently existing payment ecosystem with the new system.
6.4 Architectural Design:

The proposed framework for SPAN Wallet designed based on the software architectural standards as described in figure 6.2 which represents the enrollment and provisioning of the wallet.

![Diagram of SPAN Wallet](image)

*Figure 6.2: SPAN Wallet – enrollment and provisioning of the service.*

6.4.1 SPAN Wallet Server:

SPAN Wallet Server will act as the token service provider in the mobile payment ecosystem, where SPAN will own the wallet and manage the activities associated with this ownership such as provisioning the customer data into the mobile App once the customer initiates the process as well as taking the responsibility of managing payment tokens. The customer data get stored in the wallet server hosted at SPAN network when the customer – using his/her bank internet banking channel – enroll into the service where at that point of time the customer will be asked to provide the following information to complete the registration process: customer national ID/Iqama, card data, and a secure PIN to be used during the transaction time.

Once the customer is ready with the mobile app downloaded into his/her mobile phone, then he/she can initiate the provisioning service where the SPAN wallet with all configured bank
Mobile Payment in Saudi Arabia

cards will be downloaded into the mobile in a form of payment tokens that consists of Token number, Token expiry date, Token PIN and cryptogram with the following structure:

- **Token Number (7 digits):** generated securely by the token service provider which will be unique to each issuer bank and card number.
- **Token expiry date:** will carry the expiry date provided by the card issuer.
- **Token expiry time:** this value will carry a time interval in seconds to ensure security of the generated token.
- **Token PIN:** this will be the encrypted PIN number selected by the customer during the registration process.
- **Cryptogram:** an encrypted value which will be required to be passed during the payment transaction for wallet authenticity assurance.

SPAN Wallet Server will consist of two main components as seen in figure 6.3:

- **Encrypted DB:** This database will hold the card data information received from the issuer bank during the registration of each card number. This data will be used to initiate a complete card payment authorization.
- **Token Vault:** this component will be used to generate and store payment tokens as well as mapping the generated tokens to the respective PAN.

![SPAN Wallet Server](image)

*Figure 6.3: SPAN Wallet Server*

### 6.4.2 Member Bank:

Each member bank participating in the SPAN Wallet service will be requested to interface with SPAN Wallet system via secure link.
The interface will allow the authenticated customer to register in SPAN Wallet service and choose the account/card to be configured. Below list represents the mandatory field to be collected during the registration process:

- **Customer ID number** (Saudi ID or Iqama ID): the purpose of this information is to link all cards expected to be configured in the future to one unique reference number.
- **Card data**: This will be used to initiate the payment request from SPAN to the issuer bank.
- **Mobile Number**: to be used for any one-time password requirements and any communication with the customer.

### 6.5 Transaction flow:

In the following sections, I will be describing in details the proposed flow during registration and payment to give more clarity of the end to end process including the security of the transaction and handling fraudulent activities.

#### 6.5.1 Registration:

Registration process consists of two parts, those are: enrollment through the member bank’s internet portal as described in the previous section, and a second part that starts with the downloading of the app from the relevant store depending on the OS of the mobile phone and downloading the SPAN wallet with the configured cards which can be called an activation process.

**a) Enrollment:**

During the enrollment process, the customer will follow the below steps highlighted in figure 6.4 and described in the sequence diagram in figure 6.5:

1. Customer will initiate the enrollment process via his/her bank internet banking site and select the card number to be added to the wallet and a preferred password (PIN) to be used during payment.
2. Bank will send a one-time-password (OTP) to the customer using a predefined mobile number to ensure authenticity.
3. Customer will enter the received OTP and confirm.
4. Bank will send the enrollment request to SPAN Wallet Server with the selected Card number details and PIN as well as pre-registered customer ID number and mobile number.
5. SPAN Wallet Server will create a customer record including the process of generating payment token.
6. A Confirmation will be sent to the bank carrying the reference number to be used in activation process.
7. The bank will confirm the completion of the process along with the reference number to the customer.

Figure 6.4: Enrollment Process.

Figure 6.5: Enrollment sequence diagram.
The above process defines the enrollment steps for customers, while enrollment for merchants and banks will be mandatory as following:

- All SPAN issuing banks will be required to interface with SPAN wallet server and enable their customers to enroll via internet banking services.
- All merchants supporting SPAN transactions will be equipped with a new POS application to support SPAN mobile payment transactions over NFC technology.

b) Activation:

Activation process starts with the downloading of the wallet app as per to the following steps illustrated in figure 6.6 and the detailed sequence diagram in figure 6.7:

1. Using the downloaded mobile app, the customer will be able to initiate the activation process by providing the reference number and his/her ID which will be included with the mobile IMEI number.
2. SPAN Wallet Server will verify the received information.
3. Once the information is correct, SPAN Wallet Server will personalize the wallet with all enrolled cards.
4. The SPAN wallet will be downloaded to the mobile phone with the respective payment tokens ready for future payment.

Figure 6.6: Activation Process.
6.5.2 Payment:

Now, as the SPAN Wallet is personalized into the customer’s phone, the customer is ready and equipped with the required tool to purchase at any participating merchant using his/her electronic wallet in the phone.
1. Customer will initiate SPAN wallet in his/her mobile and request to generate token after entering the PIN number.
2. A request for authorization will be sent over NFC layer to the POS carrying the Payment token.
3. POS using the SPAN wallet app will verify cryptography using already installed private key in the terminal.
4. A request for authorization will be sent to SPAN Wallet Server over existing SPAN network.
5. SPAN wallet server will verify the generated token using its wallet vault component.
6. If the token verification is successful, then an authorization request will be sent to SPAN authorization server after looking up the card data store in the encrypted database.

Figure 6.9: Sequence diagram for payment.
7. SPAN authorization server will prepare the authorization message following the currently used standard (ISO 8583) in all SPAN payment transactions.
8. A request will be sent to the card issuer.
9. Standard SPAN authorization verification will be followed to respond the message.
10. Bank will respond to SPAN based on the result of previous step.
11. SPAN authorization server will send the response message to the Wallet server.
12. Wallet server will confirm to the POS with the authorization response.

### 6.5.3 Fraudulent Activities:

In this section I will be covering three main fraudulent scenarios and how the solution is ready to handle them, those scenarios are: a) Payment using non-authenticated or non-registered card, b) Lost phone and c) Merchant fraud.

a) Non-authenticated/non-registered card:

This use case covers the scenario of manually registering card number into the wallet and initiating a transaction. In this case, the manually generated cryptogram in the wallet won’t be accepted by the POS due to the fact that the private key installed in POS application will not recognize the fake public key used to sign the payment token by fraudster.

b) Lost phone:

In case a phone is lost and the fraudster has identified the wallet PIN number as well as the phone Password. A PIN will be required to initiate the authorization request which will be validated only by SPAN wallet server, and in this case a rejection message will be sent. After three invalid PIN attempts, SPAN wallet will block this card until an authenticated customer reset the PIN using his/her bank internet system.

Also, a customer can immediately change the PIN number and download the wallet to another phone leaving the stolen or lost phone useless with no critical data or valid information to initiate a payment.

c) Merchant fraud:

This scenario is considered when a merchant is trying to re-play a transaction after the customer has left the store, in this case the token expiry time generated earlier will be already expired as the period will be few seconds only.
6.6 Framework of SPAN Wallet:

SPAN Wallet solution consists mainly of three components, those are: Mobile Wallet App, SPAN Wallet Server, and SPAN App in the POS as illustrated in figure 6.10.

![SPAN Wallet Framework (High-Level)](image)

Figure 6.10: SPAN Wallet Framework (High-Level)

6.6.1 Mobile Wallet App:

The SPAN Wallet App (figure 6.11) is considered as the user interface for the mobile payment process. The Wallet App (or the Wallet) is storing the list of the cards configured by the customer through his/her different banks’ channels with a very limited and encrypted data which is linked with the actual device where the wallet resides. The data is not sufficient without the customer PIN which is not stored as clear value at any point of time.

The Wallet communicates with the SPAN App in the POS as well as SPAN Wallet server depending on the initiated process. While connecting to SPAN wallet server will be via 3G/4G networks, the SPAN App in the POS will be communicating with the Wallet via the NFC channel to facilitate the payment process as described earlier.

Figure 6.11 below consists of four main components required for the mobile wallet to communicate with the SPAN POS those are:
• Security Manager: this interface is protecting the wallet app and ensuring data encryption.
• Device Information Manager: is handling the mobile handset information where IMEI will be required to be retrieved for activation and payment authentication.
• Communication Manager: establishes the communication with the NFC controller in the device.
• NFC Controller/NFC Antenna: part of the NFC components in the device to facilitate mobile-POS connectivity via NFC network.

![Figure 6.11: SPAN Wallet Framework (Mobile Wallet App)](image)

### 6.6.2 SPAN Wallet Server:

SPAN server (figure 6.12) plays a significant role as a manager of the Wallet and a hub of the overall payment process.

SPAN server interfaces directly with the POS as well as the Wallet at different point of times depending on the need and step in the payment process.

SPAN server interfaces with the Wallet via secure connection using certificates issued by the SPAN server during the activation process and downloaded along with the preconfigured wallet.
The Wallet can always communicate with SPAN server at any time in case of a need to download the wallet after a new setup is initiated or in case a new card was configured and the customer would like to update the wallet. SPAN server will communicate with the SPAN App in the POS via the existing SPAN joint network which is secured network used for all POS transactions. While the received transaction from the POS App is not in the usual format of the standard SPAN transaction however SPAN server will format a standard financial transaction and send it to the issuer whenever required.

Below figure 6.12 consists of the following components:

- Wallet interface: managing the connectivity with the wallet app in the mobile.
- POS interface: managing the connectivity with the POS.
- SPAN Authorization interface: managing the interface between SPAN wallet server and SPAN authorization server to initiate the approval/authorization request with issuer banks.
- Communication manager: responsible of sending/receiving messages to/from POS and Wallet.
- Queuing manager: is required to ensure received messages are queued efficiently for data manipulation.
- Data Interpretation and manipulation manager: analyze the received message and interface with the token manager (vault) and message formatter for next actions.
- Message formatter: reformat the message based on SPAN authorization interface constraints.
- Token manager: used to generate/validate tokens.

![Figure 6.12: SPAN Wallet Framework (SPAN Wallet Server)]
6.6.3 SPAN POS:

Existing SPAN application installed in the POS will be used to interface with SPAN server during the online transaction.

6.7 Research Validity:

6.7.1 Introduction:

In any research work, validity is an indication of how sound the research is. To be more specific, validity applies to the design of the research as well as the methodology used to conduct the research, which means that the research findings represent the expected result as part of the overall research objective.

Researches can be affected by different factors, controlling those factors that might threaten the research’s validity is the responsibility of the researcher.

6.7.2 Internal Validity:

Internal validity is affected by concerns within the study itself such as collected data. Those factors that might affect internal validity could be one of the below factors but not limited to them:

- Size of subject population.
- Time given for the data collection.
- Maturation.

In my research the systematic literature review (SLR) and the architectural framework will be within the scope of the internal validity as described below:

6.7.2.1 SLR:

- In the SLR, the standard steps proposed and implemented by Kitchenham in software engineering projects were followed to ensure solid background and basis of the research.
• Selecting the primary studies for the SLR was a major challenge with the threat of the possibility in missing some publications or overlooking proven study. However, the identified resources were the accessible ones with the expectation to cover the majority of the studies. Yet, there might be some of the lately published studies that were not included in the research.

• The analysis of the selected studies is an important phase of the SLR, hence, it has been agreed to evaluate the research protocol by the supervisor to confirm the full coverage of the available data from the selected sources.

• Success factors of mobile payment implementations is a major outcome from the conducted SLR, and the threat of missing some of those factors was identified, however reviewing the protocol and the primary studies by the supervisor will ensure an acceptable level of validation with a room of more success factors that might be specific to one or more environments globally.

6.7.2.2 Architectural Framework:

• As a way of validating the proposed framework and evaluating its correctness, the framework was discussed in details with an expert from IBM who’s working as Chief Architect and country lead in providing software solution. He is also certified enterprise architect who has broad knowledge about the financial sector and the payment ecosystem in the local market. Few suggestions were highlighted by the consultant and the same was discussed with the supervisor for feedback which has resulted in amending few sections in the proposed framework. The expert suggestions were more into having details of the SPAN Wallet Server architecture as well validating the security concerns which were covered in previous and later sections.

• The framework was built with the aim of targeting a centralized-driven payment environment with more focus on the Saudi market and local payment ecosystem.

• The framework was mainly guided by the ISO 42010 standard to ensure more structured and proven method of building the framework.
6.7.3 External Validity:

External validity is mainly generalizing the findings within different environment. Therefore, we can consider any findings to be externally valid, if the findings are extendible to other environments.

External validity can be affected by many factors such as:

- Effect of the research environment:

  The uniqueness of the local market by having a centralized-driven payment ecosystems controlled and managed by a governmental entity has influenced the final proposed framework and guided the research toward similar available environments with limited resources to be reviewed however clear result of the same experience.

- Researcher effects:

  Although the access to similar environment as the Saudi environment was limited as highlighted above, however by having enough knowledge about the local Saudi payment systems as well as the financial environment due to the day-to-day activities, the researcher was able to obtain the necessary information from the required entities and individuals and leverage on my own experience as well.

- The effect of time:

  Efforts were ensured to cover as many years as possible in selecting the primary studies; however there could be other published studies outside the time interval applied which might be missed. Also, other commercially-published papers might be also not accessible during the study which might affect the final result.

6.7.4 Architectural Concerns Validity:

In order to validate the proposed architectural framework and ensure its applicability and compatibility with the expected requirements, different approaches and steps were followed including expert opinion, interoperability and security concerns including fraudulent activities expected in payment environments. In the following subsections I will be addressing each one of these steps in more details:
6.7.4.1 Security Concerns:

Security was identified as one of the success factors expected in any implemented mobile payment solution in order to make it successful, also it is one of the main concerns in the proposed architectural framework which need to be validated as suggested in the expert’s feedback.

In order to validate security concern, I will highlight how the architectural framework will address security as an embedded design factor. The below points address security from different aspects to ensure overall secure solution:

- Using Tokenization where sensitive card numbers won’t be exchanged as part of the transaction.
- Leveraging on the currently existing SAMA Joint Network (SJN) which is already proven secure network carrying the payment transactions with almost no risk.
- Using the currently certified POS’s in the market which supports the maximum level of security required by the international schemes (VISA, MC, AMEX, ...etc).
- Using IMEI number which is unique for each mobile handset as part of the activation to ensure uniqueness.
- Registering the customers based on the pre-registered ID numbers and Mobile numbers in their respective banks which follows a very strict process in case of any required update.
- Using one-time usage tokens to avoid any duplication attempt.
- Initial customer identification by forcing all customers to complete an activation process that depends on the initial enrollment process which is basically built on top of the already registered data at banks with no chance of invalid data introduced into the new mobile payment environment.

In addition to the above security features embedded in the design, we can also validate security concerns by validating different fraudulent activities expected to take place in any payment environment.

- Non-authenticated/non-registered card:
  
  Scenario: An attempt of conducting mobile payment transaction using fake application, where the fraudster will try to clone the application in his/her mobile phone and initiate a transaction via NFC using the same structure of the expected transaction.

  Solution: This attempt will be blocked by two different security levels, POS will reject the transaction by failing the cryptography value which won’t match the expected value generated using the private/public key encryption. Also, the transaction will not be allowed at the server level due to the validation conducted by the SPAN Wallet Server against the
already stored data in the encrypted database which include the IMEI of the device used for registration.

- **Lost phone:**

  Scenario: a fraudster will use a lost phone and try to initiate a transaction with or without knowing the predefined password.

  Solution: in case of a fraudster knowing the predefined password, the customers will have the ability through their respective Banks’s channel to disable the service or block the previously downloaded wallet which leaves the fraudster clueless of the reason of rejecting the transaction.

- **Merchant fraud:**

  Scenario: a merchant will try to replay a transaction after the customer has left the store using the previously used transaction.

  Solution: such scenario will be avoided by having the one-time tokens which will result in rejecting the usage of the previously processed transaction.

- **Skimming:**

  Scenario: in this case, genuine data will be copied and used in another device to try passing the security measurement usually conducted in such scenario.

  Solution: the IMEI used in registering the mobile during the activation process will be validated which will result in failing the transaction, as the mobile app will be reading the IMEI number directly from the phone initiating the transaction.
Chapter 7. Conclusion & Future Work
7.1 Conclusion:

In this thesis, the objective was to propose an architectural framework for mobile payment application that is applicable to the Saudi market. In order to achieve this goal, a comprehensive literature review (SLR) was conducted based on systematic literature review in software engineering. The result of the SLR was mainly the success factors affecting the implementation of mobile payment applications as well as latest technologies proposed by different implementations across the world.

A full study of the Saudi payment ecosystem was also conducted to ensure leveraging on the existing environment and designing the right application for the market.

The main success factors identified in the SLR were used as main enablers in the proposed architectural framework. Those factors have acted as non-functional requirements to ensure overcoming challenges faced by other implementations globally.

Finally, a detailed architectural framework for mobile payment application was proposed covering the mobile wallet design as well the detailed message flow.

7.2 Limitations:

The proposed solution has some technical challenges that need to be assessed further and evaluated, those are:

- Security of the transaction and the possibility of attempting a successful fraudulent payment other than the addressed in this thesis.
- Support of offline transactions for better experience.

7.3 Future Work:

A detailed analysis for all the different viewpoints of the proposed solution including information, development, deployment and functional viewpoints could be considered as an extension of this work in order to have more detailed understanding of the overall architectural framework of all system components. Those detailed viewpoints will address other critical concerns such as security and performance.
Bibliography


