



# An Authentication Security and Governance Frame Work for Near Field Communication in Sri Lankan Context

A dissertation submitted for the Degree of Master of  
Science in Information Security

S K Perumbuli

University of Colombo School of Computing

2017





## Declaration

This Thesis is my original work and has not been submitted previously for a degree at this or any other university / Institute

To the best of my knowledge it does not contain any materials published or written by another person, except as acknowledged in the text

Student Name: Sampath Krishantha Perumbuli

-----

Signature

-----

Date

This is to certify that this thesis is based on the work of

Mr. / Ms.

Under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name: Dr. Kasun De Zoysa

-----

Signature

-----

Date

## **Acknowledgements**

*I would like to thank...*

My Parents, for all their support, advice and love

My Wife, Vasana Habaragoda for all the support to make this a success

My Sister, Hashika Perumbuli who did the Proofreading

My Supervisor, Dr. Kasun De Zoysa for his guidance, opinion and time

All my lecturers at the University of Colombo

Mr. Chaturaga Dias and Mr. Hasitha Danthanayarana for supporting me on the interface development

All the senior team members in Mobitel, Dialog and Millennium IT for their valuable feedback and guidance

All my Collogues for all the support and encouragement

## Abstract

Near Field communication (NFC) is one of the rising and promising technological traits, provides manner to quick range contactless communication for cell phones and other gadgets alike. NFC has grown to be an attractive research region for many researchers' due to its exploding boom and its promising applications and associated offerings. At know-how, the present-day reputation of NFC studies location is essential to maintain the advancement of understanding in NFC studies and to discover the distance among principle and practice. In this research, researcher has presented literature on Governance model for NFC as well as the Secure Authentication with Multi factor. To facilitate the analysis of the literature, the researcher endorses a research framework and organize the NFC literature into four primary categories; principle and improvement, packages and offerings, infrastructure and environment. Governance model is a main deliverable in this research where it localizes it to Sri Lankan context. Authentication Security is other main objective under this research and Two Factor is the proposed model. There were many models in the world where the Literature and the knowledge from Industry experts are blended in this research. This rigorous and holistic literature review with the objective of bringing to the kingdom-of-art in NFC layout technological know-how research gives advancement of expertise in NFC research and further research directions.

Though NFC is a booming technology in Sri Lankan context and lot of work has been done by many organizations in Sri Lanka, it is still premature compared to other real-world examples. NFC application and its ECO System are still limited to very primitive applications and the technology acceptance is very low in Sri Lanka. The general public is not enthusiastic to embrace the new technologies to make their life easy as traditional paper based work is still the dominant work flow in Sri Lanka. The Governance Frame work discussed, is very much appropriate to the Sri Lankan context. But to implement this in Sri Lanka, a strong governance body to drive the process is required. This can bring lot of benefits to the country as lot of applications can be put into a single card. To Implement Multifactor authentication for authenticity, it requires certain attitudinal changing initiatives to convince the general public.

## Table of Contents

Chapter 1 - Introduction .....	1
1.1 Background and Motivation.....	1
1.2 Aims and Objectives .....	2
1.3 RSA Algorithm .....	2
1.4 RSA Usage .....	3
1.5 Two Factor Authorization .....	3
1.6 Single-Factor Authentication (SFA) vs. Two-Factor Authentication (2FA).....	3
1.6.1 Two Factor Authorization Affiliated Products.....	3
1.7 Challenges Using RSA Multi Factor Authentication .....	4
1.7.1 CA Strong Authentication.....	4
1.7.2 Okta Verify.....	4
1.7.2 Google 2-Step Verification .....	4
1.7.3 Symantec Validation and ID Protection Service.....	5
1.7.4 Secure Auth IDP .....	5
Chapter 2 - NFC Domain Related Literature .....	6
Chapter 3 - Research Methodology & Framework .....	8
3.1 NFC Research Framework.....	9
3.2 NFC Governance Model Building Box.....	9
3.2.1 NFC Infrastructure .....	10
3.2.2 NFC Applications and Services .....	10
3.2.3 NFC Ecosystem.....	11
3.2.4 Draw backs in NFC.....	11
3.2.5 Governance Framework Model.....	11
3.3 NFC Application Domain in World Context .....	12
3.4 NFC Application ECO System .....	13
3.5 Type of NFC Apps available in the market.....	14
3.5.1 Key Success Factors in NFC Application .....	16
3.5.2 Application Use Cases in NFC.....	17
3.5.3 Application Design in NFC.....	18
3.5.4 Intelligent Retail Solutions with NFC.....	19
3.6 NFC Security and Privacy.....	20
3.6.1 Importance of Security .....	20
3.6.2 NFC Security Concerns.....	20
3.6.2.1 Eavesdropping.....	20
3.6.2.2 Data Corruption in between .....	21

3.6.2.3 Data Manipulation.....	21
3.6.2.4 Man in the Middle attack .....	21
3.7 Different Approaches in Sri Lankan Context.....	22
3.7.1 Implementation in Dialog.....	22
3.7.1.1 Features in Meal Management System .....	22
3.7.1.2 Diagrammatic view of the meal card solution.....	23
3.7.2 Implementation in Mobitel.....	23
3.7.2.1 NFC Fuel Card Solution (MFlash).....	24
3.7.2.2 MLoyalty Reward Program.....	24
3.7.3 Implementation in Millennium Information Technologies .....	25
3.7.3.1 Potential applications with MIT .....	25
Chapter 4 – Design of Solution .....	27
4.1 Proposed Governance Framework .....	29
4.2 Key Functionalities in Contactless Model.....	30
4.2.1 Service Provisioning .....	30
4.2.2 Trusted Service Manager .....	30
4.2.3 Mobile Network Provisioning / Security.....	30
4.2.4 Chipset Manufactures.....	30
4.2.5 NFC Tag Manufacturer .....	31
4.2.6 Service Providers.....	31
Chapter 5 – Implementation .....	32
5.1 Overview .....	32
5.2 Evaluate the Feedback.....	33
5.3 Conceptual Design .....	35
5.3 Features in Futuristic model.....	36
5.3.1 Inbuilt Multifactor Authentication .....	36
5.3.2 Customer Relationship Manager .....	36
5.3.3 Data Analytics Engine.....	36
5.3.4 Multifactor Authentication Application .....	37
5.3.4.1 Logging Screen .....	37
5.3.4.2 Sign up Screen.....	38
5.3.4.3 Multifactor Handling Screen .....	38
5.3.4.4 Welcome User Screen .....	39
5.3.4.5 Program Code in Nutshell .....	40
5.4 Testing of the Application.....	49
Chapter 6 – Conclusion and Future Work.....	53
6.1 Introduction .....	53

6.2 NFC Governance Framework .....	53
6.2.1. User Recommendation .....	53
6.2.2 Technology Provider Recommendation.....	53
6.2.3 Governance Body Recommendation.....	54
6.3 Multifactor Authentication Application .....	54
6.4 Recommendation for Future work .....	54
6.5 Limitation in Research .....	55
6.6 Final Conclusion .....	55
Appendix .....	56
Appendix 1 .....	56
Appendix 2.....	59
Appendix 3.....	60
References.....	61



## List of Figures

Figure 1.1: How Multifactor .....	2
Figure 3.1: Strategy for Literature Review .....	8
Figure 3.2: Framework to Build on Governance Model .....	9
Figure 3.3: NFC Device Forecast from 2010-2019 .....	12
Figure 3.4: NFC ECO System .....	13
Figure 3.5: Modes in NFC Domain .....	14
Figure 3.6: NFC Target Market .....	15
Figure 3.7: Key Success Factors in NFC .....	16
Figure 3.8: NFC Application Domain .....	17
Figure 3.9: NFC Application Design .....	18
Figure 3.10: Intelligent Retail with NFC .....	19
Figure 3.11: Intelligent Retail Payment Automation .....	19
Figure 3.12: Man in the Middle Attack .....	21
Figure 3.13: Dialog Meal Management Solution .....	23
Figure 4.1: Proposed NFC Governance Model - Level I .....	28
Figure 4.2: Contactless NFC Model .....	29
Figure 4.3: Trusted Service Manager .....	30
Figure 5.1: Multifactor Authentication Survey Results .....	33
Figure 5.2: Hardware Token Vs Soft Token .....	34
Figure 5.3: Cultural Aspect .....	34
Figure 5.4: Proposed NFC Governance Model – Final .....	35
Figure 5.5: Logging Screen .....	37
Figure 5.6: Sign Up Screen .....	38
Figure 5.7: Validate Screen .....	38
Figure 5.8: Authentication Screen .....	39
Figure 5.9: CSS Style Sheet .....	40
Figure 5.10: Configuration File .....	41
Figure 5.11: Current User .....	41
Figure 5.12: Google Authentication .....	42
Figure 5.13: Registration Detail .....	42
Figure 5.14: Validate User .....	43
Figure 5.15: User Logged In .....	44

Figure 5.16: Handling User Logging .....	44
Figure 5.17: QR Code .....	45
Figure 5.18: QR Code Validation .....	45
Figure 5.19: Validate with App .....	45
Figure 5.20: QR Code Change Sequence Code .....	46
Figure 5.21: User Logout .....	46
Figure 5.22: User Class .....	47
Figure 5.23: User Logging Function .....	48
Figure 5.24: User E-mail Check .....	49
Figure 5.25: User Name Check .....	50
Figure 5.26: User Blocked .....	51
Figure 5.27: Devise Validate .....	52

## Acronyms and Abbreviations

NFC	Near Field Communication
2FA	Two Factor Authentication
NIC	National Identity Card
PIN	Personal Identification Number
SFA	Single Factor Authentication
MFA	Multi Factor Authentication
USB	Universal Serial Bus
ICT	Information Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
OTA	Over the Air
API	Application Programming Interface
RFID	Radio Frequency Identification
MIT	Millennium Information Technology
CRM	Customer Relationship Manager
IOT	Internet of Things
TAM	Technology Acceptance Model
SAM	Secure Access Module
HSM	Hardware Security Module

## Chapter 1 - Introduction

NFC abbreviation stands for Near Field Communication. NFC Services are an emerging technology to replace lot of services that require in person presence with contactless technology. In the western world, NFC is in used in diversified areas such as Finance, Telecommunication, Retail, Ticketing, and Transportation. Since the areas, it has penetrated already required governance and Security Protocol in place, there is a need for such a model to be implemented. The biggest challenge in implementing such in local context is none availability of a governance body which can take the ownership and drive it. A Governance model is required in service provisioning as the financial services can be put into the risk if the regulatory is not there to govern. Security is the other key factor that we need to concentrate on NFC, as Application Security, Server end security, User level Authentication security as well as transport layer security are the most concern security areas. User authentication security is the most vulnerable area out of all. Multifactor Authentication is the answer for this but how to integrate it with the governance model is the biggest challenge and how to select the right multifactor product that can support.

### 1.1 Background and Motivation

There is a good potential in Sri Lankan context for the NFC based applications as such applications can be replaced with lot of time consuming / Value added services which can directly benefit the general public. Due to the wide spread of mobile phones today, the potential for the mobile phone is all in one chip. Certain projects in this area have been already started like mobile cash / E –Wallet and the security and the governance is somewhat concern.

There are multiple potential cards that a normal person carries can be replaced with this. Services can be replaced with single NFC chip or an App. For an example, Bank cards / NIC / Driving License / Privilege Cards / Loyalty Cards / Insurance Cards / Health Cards can be replaced with single chip with two factor Security in it. This research is to introduce a common governance frame work which everyone can subscribe into with the required level of security.

Dialog, Mobitel and Millennium IT are the frontiers in this technology adaptation in Sri Lanka and they have already begun few projects related to this area. [25], [26], [27]

Most NFC devices use some type of authentication to confirm that a user of the device is who he or she claims to be and to prove that the user is authorized to access the device. To prevent unauthorized NFC attempts in the case of lost or stolen devices, the user needs to be authenticated before each transaction, which adds extra burden on users. This research proposes a NFC security and Governance framework that simplifies the initiation of secure Authentication in NFC. The framework uses a combination of authentication methods such as password and a pin-code generated randomly using RSA or similar algorithm.

## 1.2 Aims and Objectives

Objective 01: The goal of the project is to introduce a governance frame work which fits to the Sri Lankan context. Currently, the NFC applications are in isolation with no governance. Security of the Authentication is based on username and pass cord.

Objective 02: Proposed model is to introduce “Two factor Authentication” which brings the security in Authentication and introduces a governance frame work which can fit into Sri Lankan context.

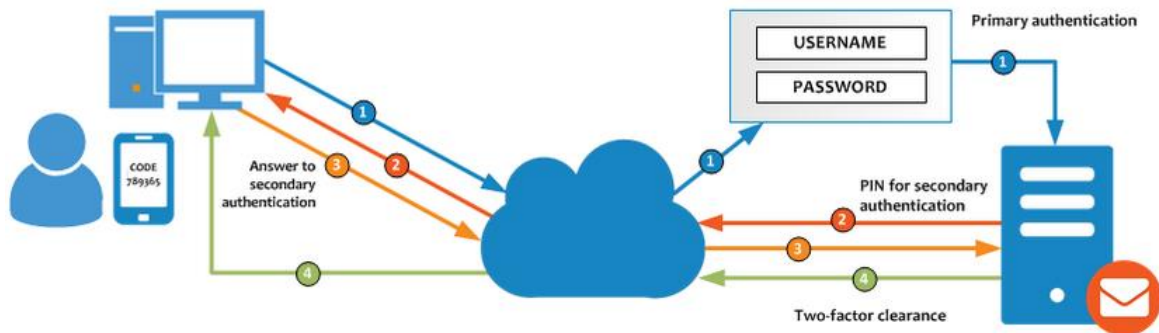


Figure 1.1: How Multifactor Works

In Summary, these are the deliverables planned at the end of this project.

1. Common Governance Frame work – This will be a platform for all applications with required level of security. Also, this will be a unique frame work for Sri Lankan context.
2. Authentication Security – Introduce Two Factor Authentication to secure the Authentication.

## 1.3 RSA Algorithm

One of the first practical public-key cryptosystems commonly used to secure data transmission is RSA. The term RSA consists of the first letters of the Surnames of Ron Rivest, Adi Shamir and Leonard Adleman who described the algorithm in 1977 (It was said to be before the 1973, an English mathematician Chifford Cocks had developed a similar system). [32]

In a cryptosystem, the public key is based on two large prime numbers with an auxiliary value. These prime numbers must be kept secret. The public key is used to encrypt a message and if it is large only knowledgeable people can decode the message. The process of breaking down RSA encryption is called “The RSA Problem”.

Nevertheless, it is not used widely as it is a relatively slow algorithm. But much higher speed, encryption-decryption operation can be performed when RSA passes encrypted shared keys for Symmetric key cryptography.

## 1.4 RSA Usage

Using the two keys namely a Public Key and Private Key, RSA algorithm involves three steps; Generation of the Key, Key Encryption and Key Decryption. The public key is open and the private key is secret. Encryption using the public key is a simple task whereas the decryption using the public key demands higher capacity. When the factorial problem is hard, the power and security of the RSA cryptosystem is higher. Currently, it is accepted that the full decryption of the RSA cipher text is not possible due to the unavailability of efficient algorithm.

## 1.5 Two Factor Authorization

The security process in which the user provides two means of identification using two separate categories of credentials is commonly describe as “Two Factor Authentication”. Out of two factor one can be a token may be the form of a digital card (Like HSBC Hardware Token for Bank Logging verification) where as another credential is a memorized chunk more like to be a security code. Best example for two factor authentications is a bank card; physical item being the card and the personal identification number (PIN) being the memorized security code. Without both the physical material and memorized material, access is impossible. This will be challenged now as most of the banks allow you to withdraw money with Single factor as ID number can be the only factor that needs to insert to withdraw money.

As the proponents suggest the ability to reduce occasions and identity theft, phishing expeditions and other frauds are higher when using the two-factor authentication as one credential alone is not worth enough.

## 1.6 Single-Factor Authentication (SFA) vs. Two-Factor Authentication (2FA)

Single factor Authentication is based on one common factor may be knowledge in the case of an ID and password. It happens to be a popular form of SFA due to the low cost, ease of implementation and familiarity. This ID and password are not secured. Multiple challenge response questions and standalone biometric verification methods can provide higher security than single factor authentication.

Password based authentication requires strong memory and knowledge to memorize it and protection from possible internal threats in the form of carelessly discarded password notes, Old hard drives and social engineering exploits. They also become victims of external threats like hackers dictionary or rainbow table attacks. As attackers, can break into password based security system of protected as well they are equipped with resources. In this case two factor authentications allows additional security.

### 1.6.1 Two Factor Authorization Affiliated Products

Large variety of devices and solutions use two factor Authentication in operation today. The range is from token to RFID cards to smart phone apps. With the current penetration of smart phone devises, cards will become none popular in near future. An Application becomes number one contender for 2FA in the future.

- RSA Secure ID is the most common multi factor at the moment.

- Google Authenticator recently became popular with the introduction of Google Pay and I-Pay by Apple.
- Microsoft Phone factor offers a reasonable cost or free of charge to penetrate the market and they are more focus on Enterprise business.
- Dell Defender is a multifactor authentication which allows token as well as Biometric.

## 1.7 Challenges Using RSA Multi Factor Authentication

RSA is a commercial product and it is hard to get a free evaluation even for 30 days to test the scenario. They have given a price quote of \$ 500 for a free evaluation which is beyond the acceptable limit. So, there is no other option other than looking for an alternative product which can support the Multi factor authentication for NFC Application authentication.

There are few products that can support the multi factor authentication which can be tested freely. Some of the available products listed in previous sections and commercial products will be discussed below.

These are the alternatives available to subsidize the RSA Multifactor.

### 1.7.1 CA Strong Authentication

CA Strong Authentication is found in both windows version and a Software as a service version namely CA Secure Cloud. It consists of the ability to configure policies, monitor activities and investigate suspected attacks. Thus, it makes it easier to track tokens and understand about the applications which support tighter MFA Security, Strong Authentication functions, authentication methods including two factor authentication software tokens. Furthermore, it helps organizations to discard passwords.

### 1.7.2 Okta Verify

Okta Verify is an MFA and SSO product. Functioning as an MFA tool, it measures standard username / password logins and variety of servers' services. When it functions as an SSO tool, it lets end users to sign into a web-based portal that serves as the basis of the authentication of an organization's SSO app portfolio. Okta verify differs from other MFA products as it has a unique feature called "Just in time provisioning", which allows authenticating with Active Directory accounts on the fly. Therefore, when the users start to use the SSO components, OV can try to construct their accounts on the fly.

### 1.7.2 Google 2-Step Verification

Two step verification code generated by Google is called the Google Authenticator. This is becoming very popular among the users as user collaboration is very high. Two-step process means second challenge apart from one's google password. Since it is a random generated number from the app installed in one's phone, it provides a multi-step security process that makes the security stronger.

Features

- App can work off line, without internet connectivity
- Easy integration with many applications and providers

- Available in all market places such as Androids, Apple and Windows
- Can get it as SMS for one's phone
- In case of compromise one's account, it has the facility to get the verification code to one's backup phone number
- Voice mail facility to get the verification code
- Facility to use Security Key instead of the code as a USB Blogger

### 1.7.3 Symantec Validation and ID Protection Service

Symantec has ruled the MFA market for a considerable period. Symantec Validation and ID Protection Service support a wide range of hardware and software including desktops and smartphone apps. Furthermore, the credentials of Symantec are used to authenticate more than 100 different websites and integrated more than 30 different common apps

### 1.7.4 Secure Auth IDP

Secure Auth Idp is both a multifactor and a single sign on authentication product which is unique. It offers an array of MFA features including support for multiple hardware and software tokens. Furthermore, it allows organizations to connect with directory services namely Active directory to allow users to sign into a web-based portal.

For this research, selected Google Two Factor Authentication as second factor for authentication process simply because of the following reasons.

1. Easy to adopt as almost all the people now own a smart phone
2. Easy to manage as seamlessly working
3. Perfect Pool proof solution
4. Support is available
5. Apps are available in any Market place
6. Hard token is not required to demonstrate



## Chapter 2 - NFC Domain Related Literature

In this globalized world, fast technology facilitates commercial enterprise drastically. The invasion of e-commerce has introduced notable developments in the form of contactless technology. Thus, near Field Communication (NFC) has gained the status of a remarkable technology tendency in ICT industry.

NFC is a short-variety, high frequency, low bandwidth and Wi-Fi communication preliminary based on Radio Frequency identity technology which allows the transferring of facts within few centimeters' radius.

NFC is specialized for its simplicity (Madlmayr et al. 2008) which attracts a large audience. Many NFC enabled applications and offerings are advanced which run in three special modes; Reader – Author, Peer to peer and Card Emulation. Furthermore, the integration of the NFC technology into all gadgets have created attractive packages in Charging, Ticketing, and Loyalty Services, Identification, Content Distribution, Smart advertising and marketing. As NFC is characterized for exploding boom, promising packages and associated services it has become an important study area considerable percentage of NFC studies are presented a Layout science studies (Havner et al. 2004) suggest the distinction of behavioral science and layout science research.

Design technological – know-how is a problem-solving method which creates and evaluates facts related to identify organizational problems. Their knowledge on the importance of design technology in IT system research areas is remarkable. They provide important hints for researches to gain knowledge on strong design technology research in information structures. (IS) Thus creating an efficient NFC design technological know –how is an important difficulty. Contemporary NFC literature is considered to be a layout technology than a behavioral technology.

Reviewing literature related to NFC e-commerce (digital commerce) is also worthwhile. It has become popular due to its novelty. Presently e-commerce has a huge demand in the market as many enterprises are interested in it. According to Ngai et al. (2002) and Wang et al. (2007), e-commerce is studies under four dimensions namely programs, generation, assist and implementation, other troubles. In addition, comparative analyses show an impact on problems and destiny research areas. As Hevner et al .2004 show, most of the study papers are based on improving rigorous research strategies of articles and further empirical studies, which can be used as a guideline for layout technology researches.

Literature related to cellular commerce (m-trade) is also significant in relation to NFC studies. According to the studies carried out by E. Ngai et al. (2008), the gap between concept and practice was recognized and suggest guidelines for E-commerce, through a properly structured classification framework and analysis. Another related study area for NFC is Radio Frequency identity (RFID) which has a close relationship. As shown by E. Ngai et al. (2008), RFID includes technological troubles, application regions, coverage and protection troubles and other issues. This observation is of vital importance for researches.

Near Field Communication is very effective when it comes to the short-range communication as per Hasleteiner and Breitfub. NFC has evolved around contactless technologies and its' ECO system & Stake holders. Beauty of NFC devises are, it can both receive and transmit data simultaneously as per Agarwal P. (2012) shows. Technology is not shifting towards both NFC and M-Commerce as per Lindon A. & Fenn J. (2003). This is simply because of the rise of smart phone & Tablets. This allows E-Marketing to widely consider NFC as their integration partner for various transaction based systems. Rise of NFC works positively on mobile industry

as well. With the hype of smart phone due to its advantages such as technology adaptation, NFC industry boosted as rich infrastructure world wide support their business model as per Falko O., Rukzio E. (2007).

NFC has become a key stake holder in Electronic Payment systems with its benefits as per Ortiz, S. (2006). It took little while the ECO System to standardize and to make sure the backward compatibility is achieved as per Moscozo, O.Z., Lekse, D. (2012)

The literature review on NFC would provide a strong foundation for data analysis of the research. As shown in the literature review, the previous studies done on NFC technologies provide useful insight to this study.

## Chapter 3 - Research Methodology & Framework

The aim of this study is to understand NFC research as a design science research area by examining the current literature to provide insights for NFC practitioners and researchers. Since NFC is a rather lately emerging technology, research papers on NFC are relatively recent, so that the first NFC related papers are published starting from 2005. Scope of the work in this research is bound with the time frame of 2006-2016; this time span covers the NFC literature.

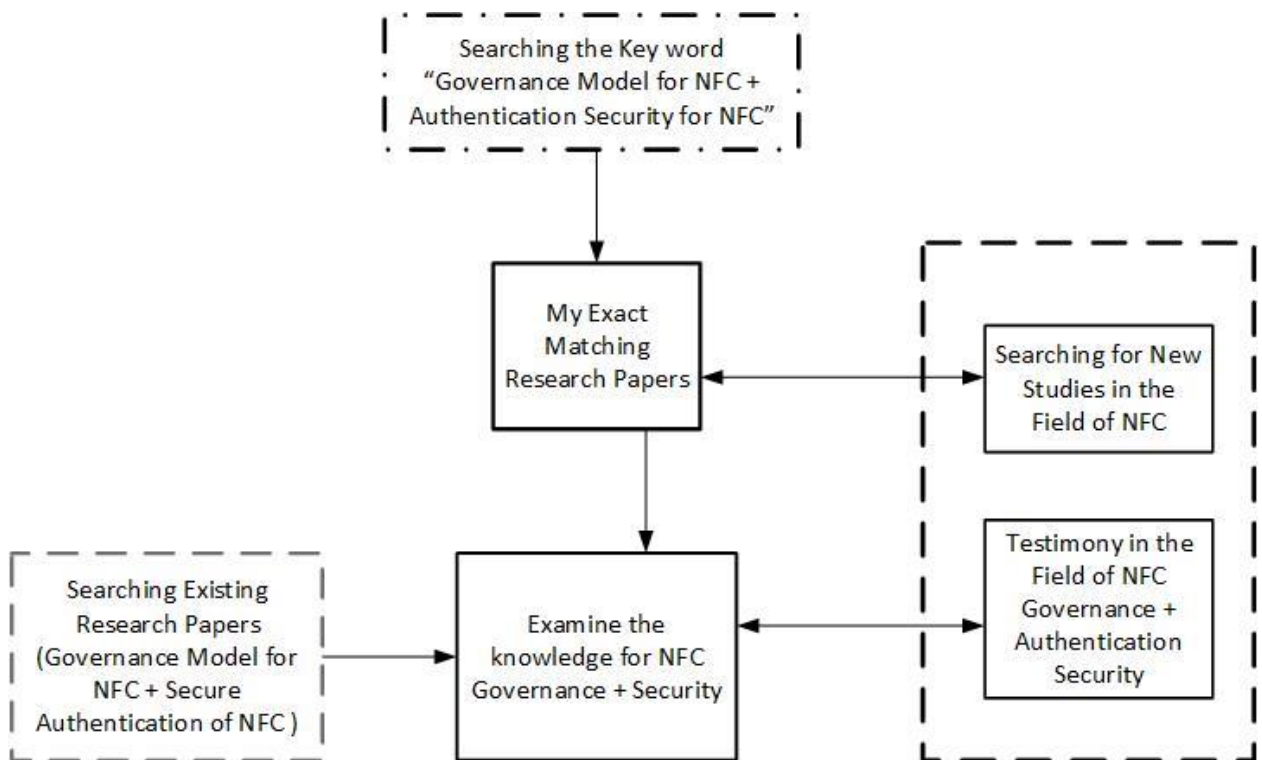


Figure 2 : Strategy for Literature Review

Figure 3.1: Strategy for Literature Review

After performing the search for the papers as defined above, the researchers have found 16 articles directly related to the subject domain in NFC. The literature search is based on two descriptors; “NFC Governance” and “NFC Framework”. It is conducted using the following electronic databases:

1. Google Scholar
2. IEEE/IEE Electronic Library
3. Academic Search Complete
4. Science Direct
5. Emerald Full Text

Sometimes the abstract, but mostly full text of each article was read to identify whether the article has tight relationship with my research topic. The literature review strategy followed for this study was an iterative process as data classification related to NFC was search in iteration. The researcher tried to find and add new studies about NFC. In doing so, the researcher can provide academics and practitioners with a comprehensive base for better understanding of NFC research.

### 3.1 NFC Research Framework

The Proposed NFC research framework includes a content-oriented classification (Ngai et al. 2008) of the NFC literature. NFC literature can be mainly put into four major baskets (Figure 3) and signified the tight correlation between each other: NFC Theory and Development, NFC Infrastructure, NFC Applications and Services and NFC Ecosystem.

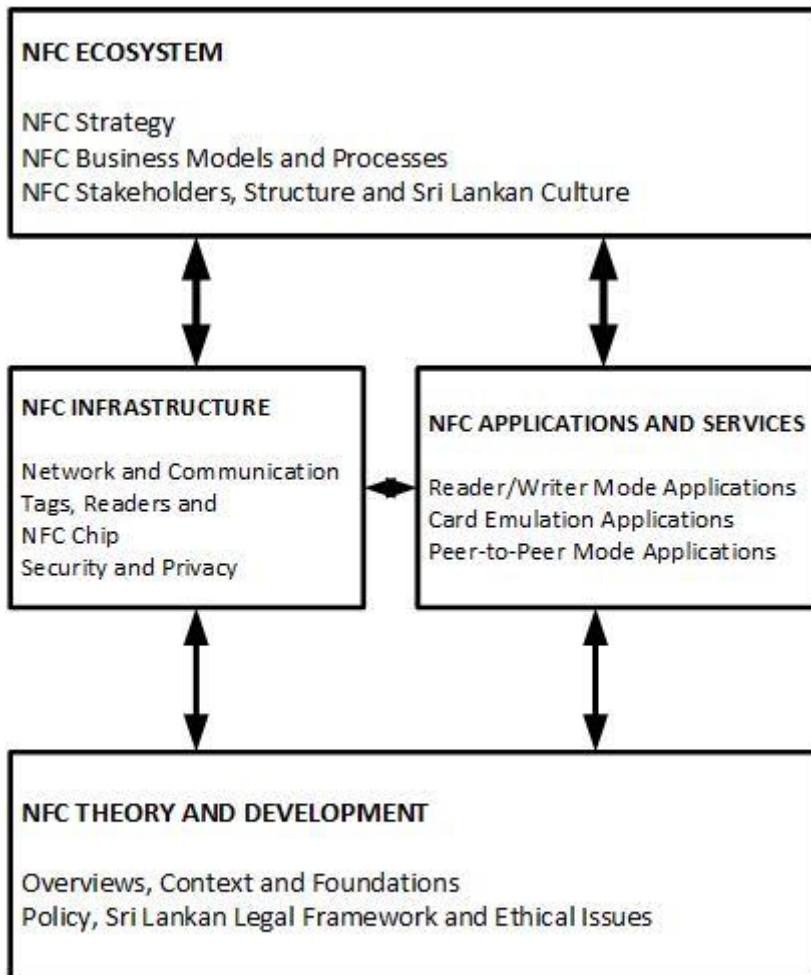


Figure 3 : Frame work to Build on Governance Model

*Figure 3.2: Framework to Build on Governance Model*

### 3.2 NFC Governance Model Building Box

The fundamental level of proposed NFC research framework includes studies related to the development of NFC technology and applications. It is studied under two aspects.

The aspect of ‘Overviews, Context and Foundations’ include general introductions, assessments, reviews about NFC, standards of NFC technology, performance analysis and measurements and new guidelines for further development of NFC enables applications and service. The second aspect, ‘Policy, Legal and Ethical Issues’ includes security, privacy, legal requirements, rules and regulations.

### 3.2.1 NFC Infrastructure

This level is discussed under three aspects

1. Network and communication issues –data related aspects, OTA transactions, New commerce protocols, New Product offering
2. Hardware issues –tags, antennae, Reader and NFC chips
3. Security and Privacy Issues –How to manage CIA (Confidentiality, Integrity and Availability)

The focus is to develop design artifact rather than behavioral issue.

This level is related to existing technology infrastructure, applications and existing ecosystem. Thus, the NFC infrastructure related research supports new entrepreneur need due to the search process of it.

### 3.2.2 NFC Applications and Services

NFC enabled Apps and services are in the mid-level of NFC framework. They are affected by other levels and give a problem space or new business needs. The available wide range of NFC applications provide prototypes with rigor design artifact evaluations namely experiments, testing and field studies. NFC applications can be divided based on their operating modes.

- a. Reader/Writer mode applications –devices used to read and modify data store in NFC transponders without batteries
- b. Card emulation mode applications-devices behave like smart cards i.e.-payment and ticketing
- c. Peer – To-Peer mode applications-link between two devices to communicate, exchange data.

### 3.2.3 NFC Ecosystem

The highest level of NFC Research Framework is the NFC Ecosystem. As it is a part of the problem space of NFC research, the changes in mid and fundamental levels directly affects NFC Ecosystem.

NFC Ecosystem can be examined in three categories

- a. NFC Economic and Strategy
- b. NFC Business Models and Processes  
Deal with business requirements, analysis and Management of NFC Tech
- c. NFC Stakeholders structure and culture – deal with the social aspect of NFC Technology namely roles, characteristics and capabilities (i. e. reliability, adoption, usability, acceptance of stakeholders in the form of MNO, service providers and end users and finally the culture of NFC enabled services. The role of the stakeholders in NFC research and development is significant. According to Hevner et al. (2004) the NFC Ecosystem includes tasks, problem, goals and opportunities of business needs which are perceived by the stakeholders. The above-mentioned perceptions are modified by the potentials of the stakeholders. They are evaluated in the economic and strategies background, structural and cultural background and business models and processes.

### 3.2.4 Draw backs in NFC

Since NFC is a commercial product, certain drawbacks and limitations are there when it comes to testing. They have base rules set to open their API for testing as they need financial gain on products, which is understandable. In this design, the researcher has evaluated NFC multifactor as my security Authentication product and the design and model was done based on NFC. But when it comes to implementation, the product is not free of charge as they need a commitment and deposit to start the testing. The researcher has tried out all the possible options to negotiate with them on the testing but all are miserably failed.

### 3.2.5 Governance Framework Model

Governance is a common principle related even to IT. Based on performance and risk management, IT governance acts as a sub discipline of corporate governance. It is necessary to guide and provide best interest of all stakeholders uplifting the quality performance and value of the organization in the competitive world, Principles of Scientific Management, Total Quality Management and ISO 9001 quality management had laid the foundation for IT governance.

During the past IT decisions were taken by the board level executives excluding the IT management. That created conflicts within the interests of other stakeholders. But when based on IT governance, that hindrance is removed and all the levels including board members, executives, staff, customers, communities, investors and regulators are in involved improving the responsibility.

As a result of IT governance frameworks identify and links all the levels to use information and related technology to manage risks associated with IT and improve quality and value.

### 3.3 NFC Application Domain in World Context

NFC has gained a significant market share worldwide over past couple of years. Since the technology is declared as an easy to use technology model, can be used for many application dimensions. Main motivation behind NFC success is integration of personal and private information such as credit cards, Privilege cards in to a personal mobile. As per ABI Research in their latest published in 2015 projected 200% penetration in next 4 years.

Chart 1: NFC-enabled Product Shipments by Product Category  
World Markets, Forecast: 2010 to 2019

(Source: ABI Research)

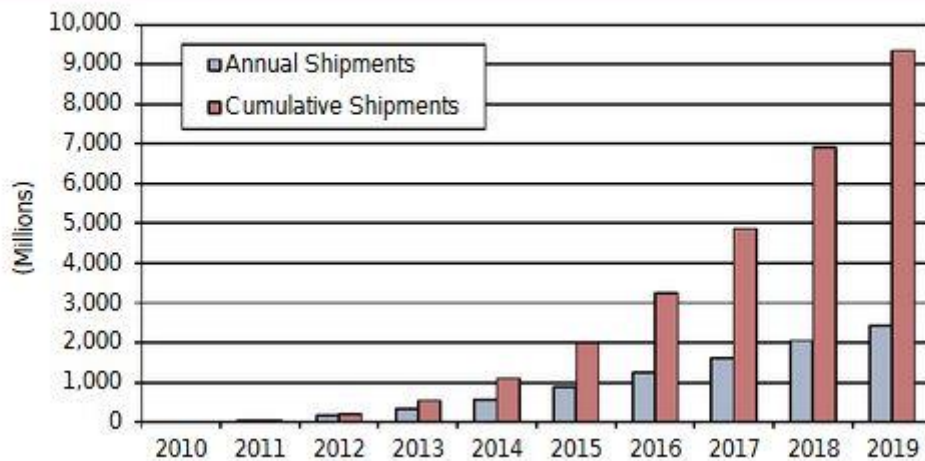


Figure 3.3: NFC Devise Forecast from 2010-2019

Key drivers in exponential growth path in NFC

- Mobile payments govern by the global player like VISA and MASTER
- NFC will be bridging between wireless technologies or paired with it
- NFC will continue to be cheaper in the market which was very expensive in 2010.

### 3.4 NFC Application ECO System

Below are the main Stake holders in NFC Application life cycle. They play a key role in NFC success in all departments. Below diagram further explains the stake holders in ECO system in detail. Application security is one of the key factors that will contribute the large penetration in NFC.

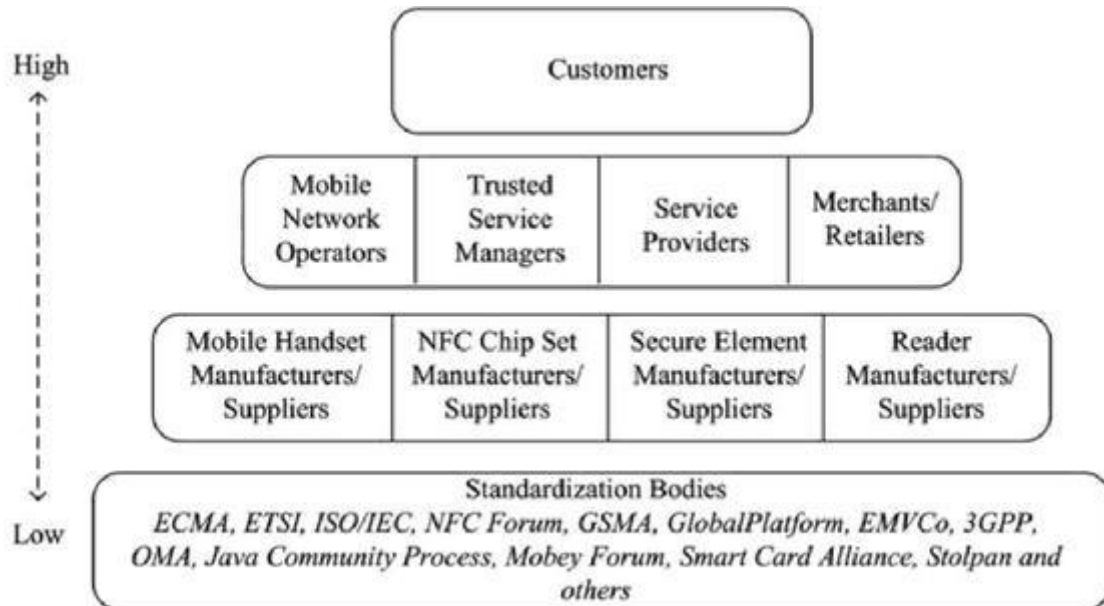


Figure 3.4: NFC ECO System



### 3.5 Type of NFC Apps available in the market

Some of the solutions that are running currently in the NFC in world context must be paid attention to. In the European region and United State of America, these services are very popular.

NFC Applications fall into one of the below categories.

1. Card Emulation Mode
2. Peer – to – Peer Communication
3. Reader Mode

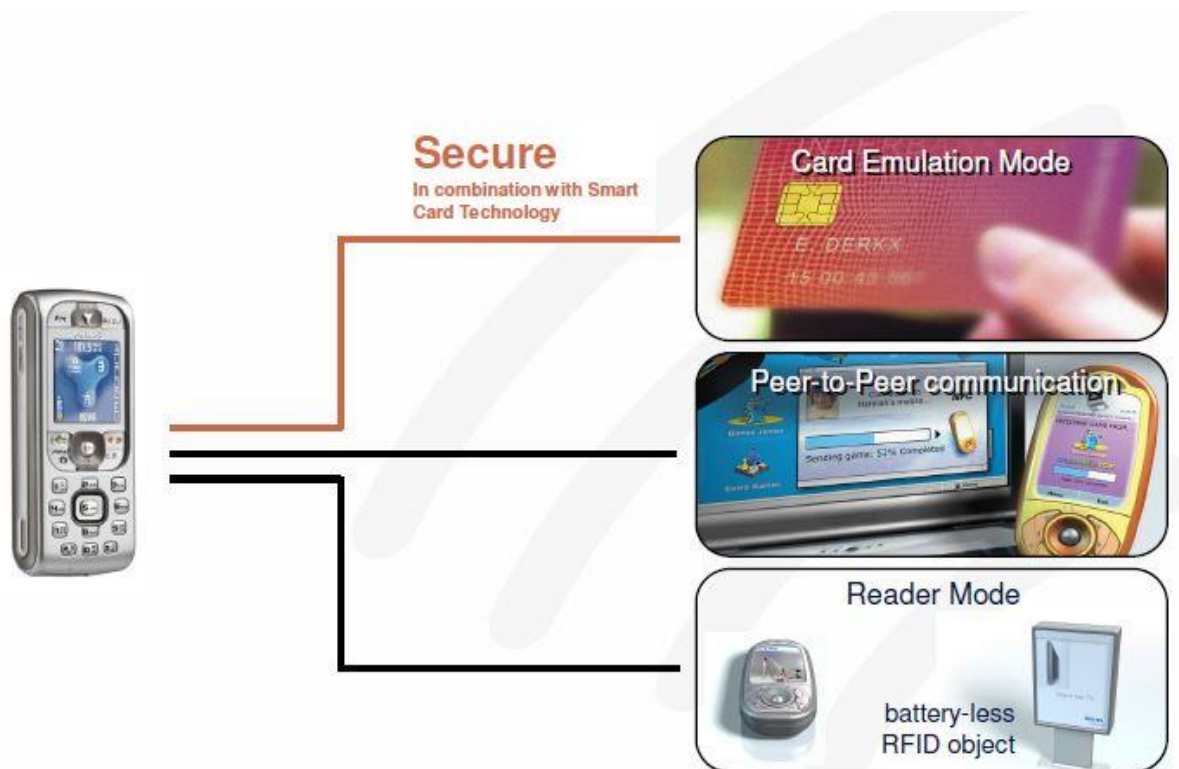


Figure 3.5: Modes in NFC Domain

The counties which have penetrated to NFC are in couple of main domains. These domains are not restricted but based on the cases available, these are most popular. This does not mean that these are the only domain that can be played by NFC.

1. Mobile Market
2. Consumer Electronics Items
3. Communication Connector
4. Logistic and retail



Figure 3.6: NFC Target Market

In modern era of electronics, one can find all come with NFC enabled. So, the traditional NFC tags will be slowly moving out and the price of the tags will become cheaper.

### 3.5.1 Key Success Factors in NFC Application

There are many factors that can determine the success of the NFC application. Timing will play a major role as some of the ground-breaking initiatives have failed due to bad timing.

Ex: E-Money order service invented by Dr. Kasun and eventually a failure because of the bad timing it lounged.

Also, one needs to consider Technical, Business Case, and Usability of the application as well as the Legal frame work that can sustain in the country.

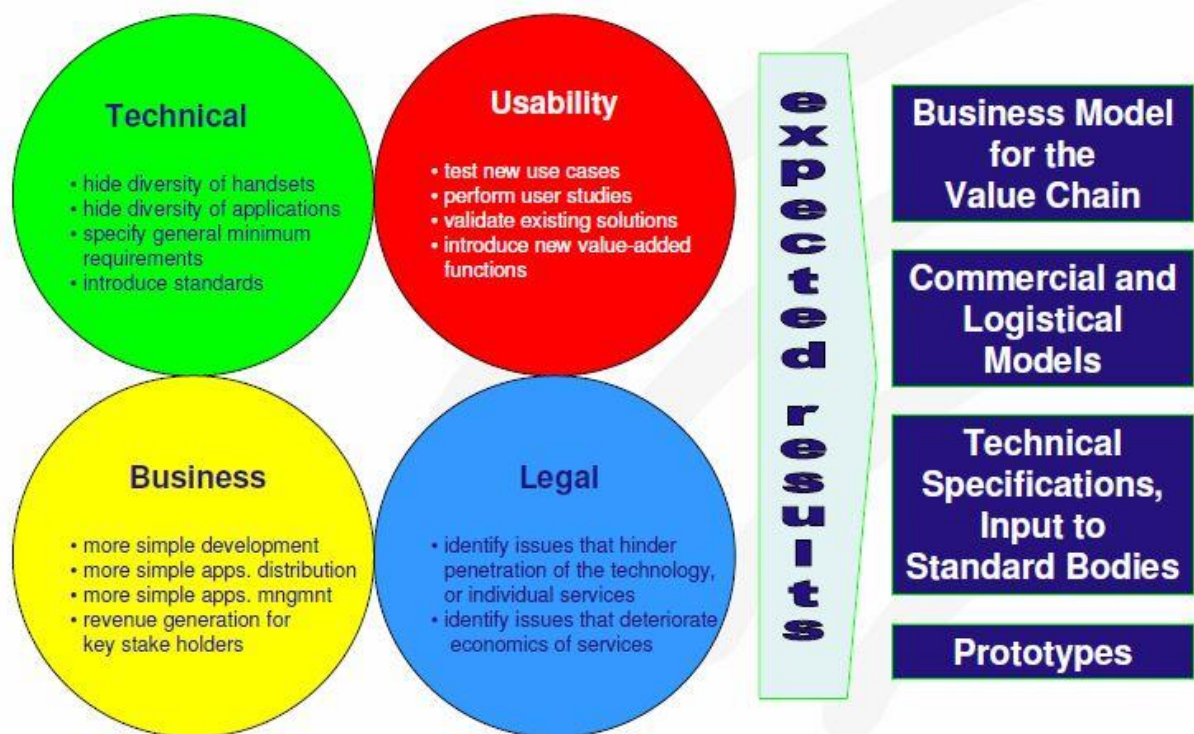


Figure 3.7: Key Success Factors in NFC

It is not just the technical factors that can go with an application but also the above factors play a major role.

### 3.5.2 Application Use Cases in NFC

As stated in the above chapter, there are many domains that were captured by NFC. Some are sole players in NFC while others give a good run to other technologies such as RFID.

Main domains that NFC are playing

1. Payments (Mobile, Credit Cards, etc.,)
2. Connectivity (Consumer Electronics, Digital Right Management, etc.,)
3. Ticketing (MRT Stations, Trains, Subways, Public Transport, etc.,)
4. Access control (Physical Control, Right Management, Identity Control, etc.,)
5. Loyalty Cards (Privilege Cards, Air Line Cards, Health Insurance Cards, etc.,)

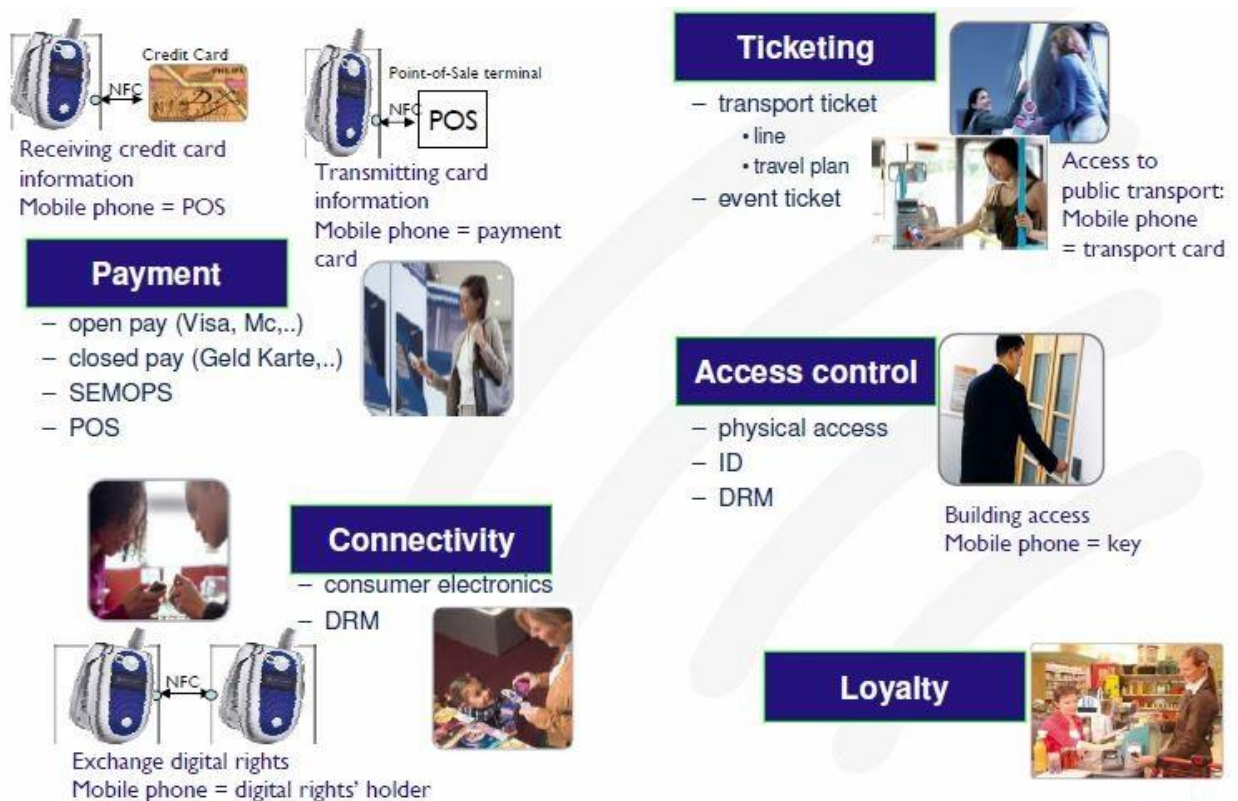


Figure 3.8: NFC Application Domain

### 3.5.3 Application Design in NFC

It is important to touch on some of the design principles of most popular applications. This will be useful later when we discuss about the NFC Security factors and how we can adopt these factors in Sri Lankan context.

This is how the ticketing application & Mobile payment Applications work in nut shell.

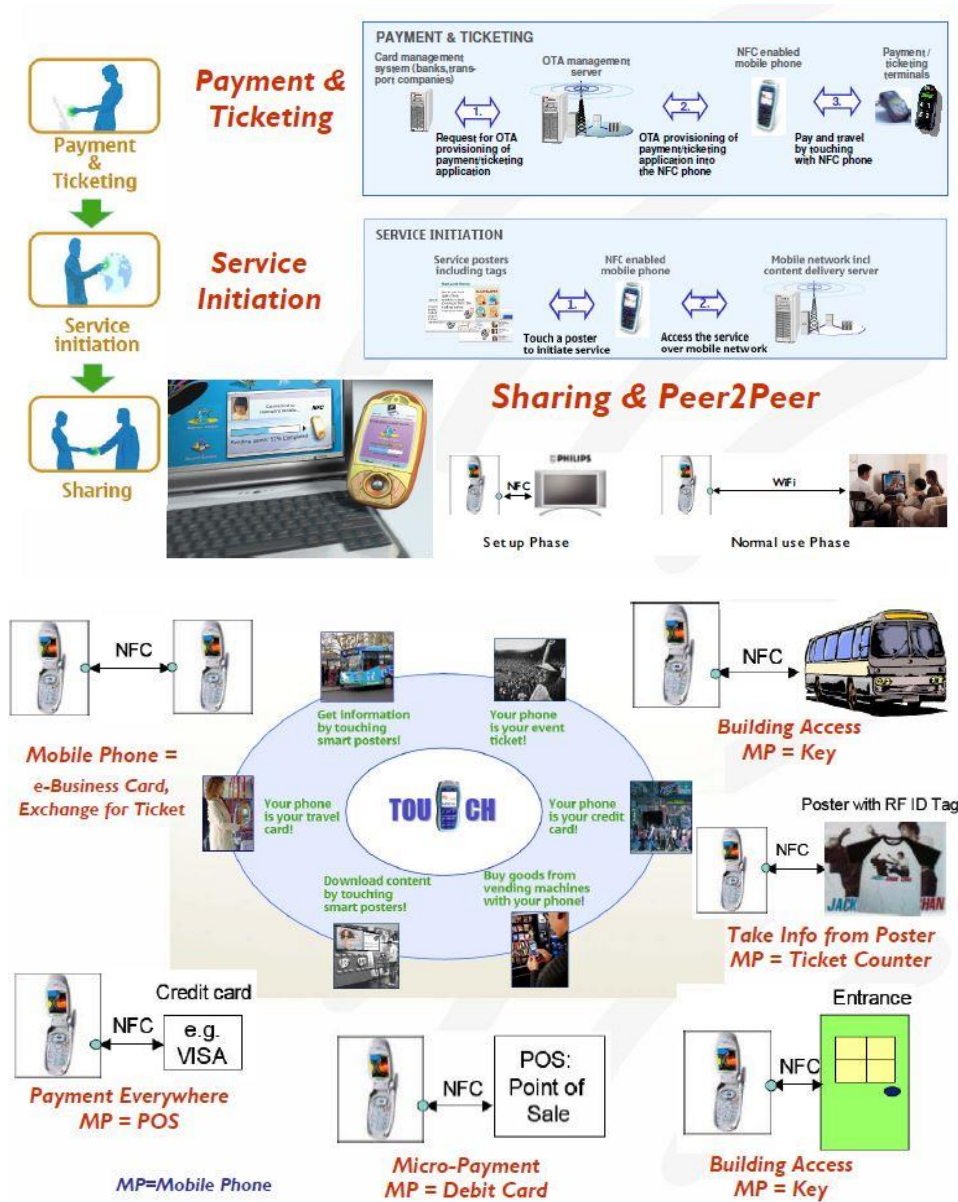


Figure 3.9: NFC Application Design

### 3.5.4 Intelligent Retail Solutions with NFC

Further to the application stack, we can have Intelligent Retailing solution that can automated lot of manual work in retail stores

There is a huge potential to automate below retails store location with smart NFC application with right security.



Figure 3.10: Intelligent Retail with NFC

Last but not least, Retail payment process can be automated with NFC

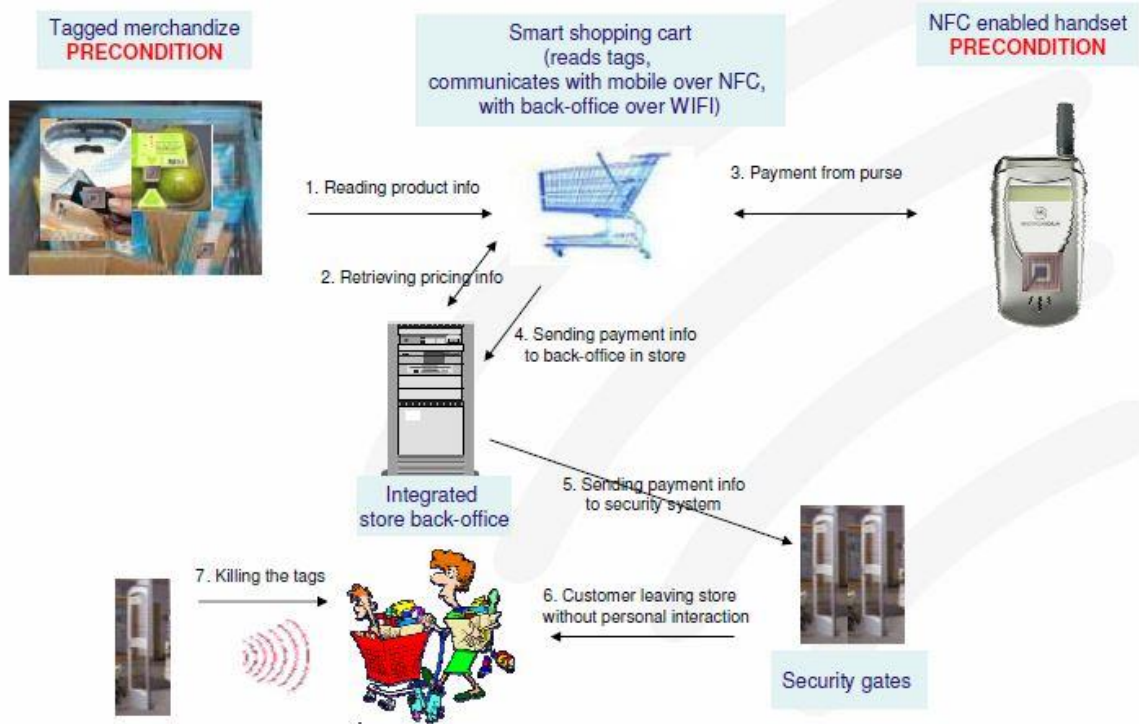


Figure 3.11: Intelligent Retail Payment Automation

## 3.6 NFC Security and Privacy

In the context of this research, NFC Security plays a vital role. NFC is mostly now coming in build with Smart phones, not a difference between personal PC and a mobile phone. Security in terms of physical devices as well as technical aspect is important. People believed to be most concern about the physical security of the mobile phones such as theft technical attacks such as Bluetooth attacks wireless attacks are still highly possible. Also, the integrated capabilities in NFC have also given a boost for attackers.

### 3.6.1 Importance of Security

Service what matters to the user but realizes the importance of the Security subsequently. In a nut shell service is useful only when the function and security both goes hands in hand. Technical limitation and the Security loop holes are the main turning points of service being popular or not. Security becomes a notable component sometimes back when the users learn the lesson in hard way. When the cost of the damage is too large, people will realize the importance of security but then it is too late.

There are many reasons why the red alert is alarming recently.

1. People who do the damage will gain financial gains.
2. They satisfy themselves or boost themselves.
3. They may be the headline of the society and become famous characters.
4. Total numbers of users expose to internet is increasing day by day so it is difficult to control
5. Due to the fact that financial asset has increased, the motivation is high for the bad guys.
6. Typical organization has not given prominence to the security usually as their business motive is sales target or the financial numbers.

### 3.6.2 NFC Security Concerns

There are few main Security concerns in NFC. When using the NFC applications, one should be aware of the pitfall associated with the technology.

- Eavesdropping
- Data corruption
- Data modification
- Man-in-middle attack

#### 3.6.2.1 Eavesdropping

Even NFC is working in short range (below 15 cm) vicinity, this cannot immune to hacking threat. Since NFC uses wave to communicate and it is possible to jam the signal transmitted. To receive the other party signal strength, need to be certain limit, eavesdropping cannot be eliminated. An attacker may use high end antennas to receive the signal so the only way of eliminating is to encrypt the signal.

### 3.6.2.2 Data Corruption in between

There can be a possibility to block the legitimate traffic by the attacker by sending bogus traffic blocking the legitimate traffic to flow. This way the legitimate data may be corrupted in the middle. This attack is commonly called Denial of Service attack. To lounge this kind of attacks, the attacker needs to have a powerful transmitter which can be identified by the NFC device if we have the right security in place.

### 3.6.2.3 Data Manipulation

The attacker can have a powerful device arranged to receive the transmit data and manipulate in between and broadcast. This is possible when the data format is not changed and only the bit level changes have done. Data encrypt and transmit will be the way of protecting against this kind of attack.

### 3.6.2.4 Man in the Middle attack

This kind of attack is possible when the third party intercept the communication and relay the data without modification. So, the original party will receive the data as it is.

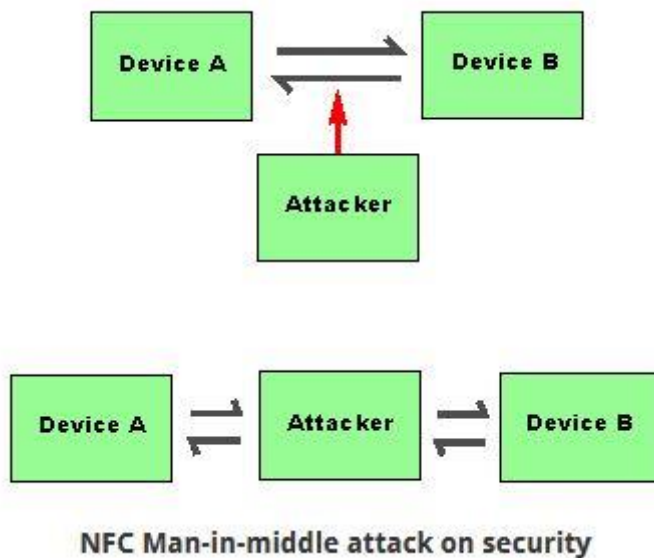


Figure 3.12: Man in the Middle Attack



### 3.7 Different Approaches in Sri Lankan Context

In Sri Lanka, only a handful of companies is in the NFC domain. Out of which Millennium IT, Dialog Axiata and Mobitel are the three leading players. The researcher has studied all of their design and implementation methodology to understand the common architecture and framework that can be implemented.

In this chapter, the differences between two main architecture and implementation are discussed.

#### 3.7.1 Implementation in Dialog

Dialog Axiata is the leading telecommunication service provider in Sri Lanka which has more than 8 million subscriber base in Sri Lanka. They have gain more than 50% of the market share in Sri Lanka and more importantly they have penetrated in other services such as online purchase portal (wow.lk), Satellite television (Dialog TV), Online Sport Entertainment (papare.com). These are some of the few of what they are in the business. They are one of the largest service provider in NFC specific application such as Fuel cards, Loyalty cards, Meal management Systems, Attendance Capturing System. They are controlling a significant portion of the NFC applications in Sri Lankan context.

The researcher has taken an approval to sight some of their product under this chapter only for the research purpose.

Two main products they market here are

1. Meal Management System
2. Corporate Fuel Card

##### 3.7.1.1 Features in Meal Management System

This product is to manage the meal counting solution for large corporate offices. The Solution has gone beyond the meal counting and provides you the end to end Canteen management solution with NFC technology.

1. Staff Meal Card – A pre-paid card (with / without a ceiling limit)
2. Executive Meal Card – A post-paid card (with / without a ceiling limit) Excess usage will be deducted from employees at the end of the month
3. Senior Manager Meal Card – A post-paid card (unlimited)
4. Visitors (Outsiders within the group) - Limited transactions for limited time period

### 3.7.1.2 Diagrammatic view of the meal card solution

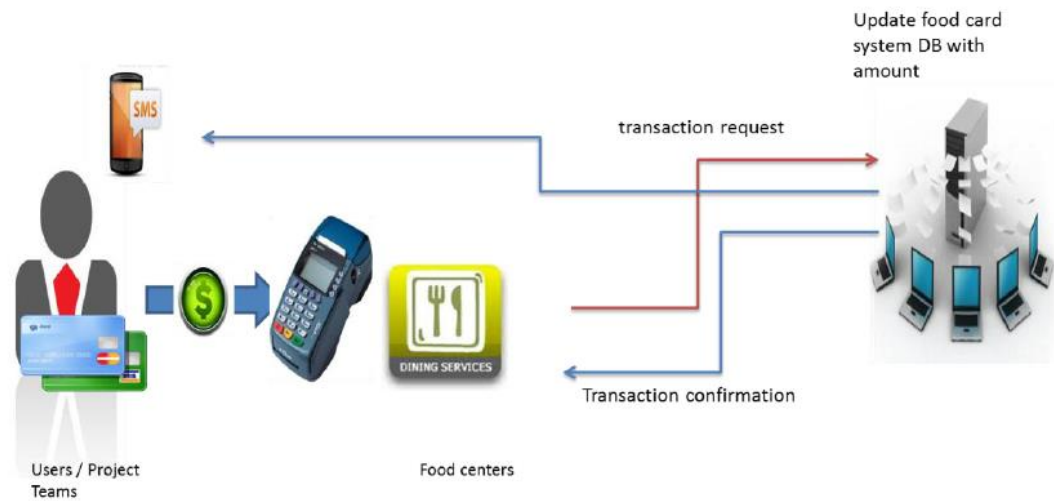


Figure 3.13: Dialog Meal Management Solution

### 3.7.2 Implementation in Mobitel

Mobitel is the national service provider where the parent company is Sri Lanka Telecom. Mobitel started its' operation in 1993 in Sri Lanka and expanded its' services to wide spread of areas in Solutions. They are in money service called "Mcash" which is their signature product now apart from the mobile services.

In the area of NFC, Mobitel has also gained a significant ground in Sri Lankan market as they are very quick to react to the market trends.

Currently following services are in offering from Mobitel.

### 3.7.2.1 NFC Fuel Card Solution (MFlash)

Mobitel has tied up with both Indian Oil Company and Sri Lanka Petroleum Cooperation to have a wider spectrum of Coverage Island wide. They have onboard more than 100 fuel stations at the moment in Sri Lanka.

Following are their objectives with MFlash Solution.

Features

- Fast transaction via secure offline mode
- Minimize manual inconveniences of fuel administration
- Easy tap and go method saves time
- High Operational efficiency
- Reduction of cost in over head
- Instant SMS notification on transaction
- Provide web interface for company administration

### 3.7.2.2 MLoyalty Reward Program

MLoyalty is frequent reward program designed to cater for relationship marketing. This can be customized as per your needs to strengthen the relationship with your customers. MLoyalty is running on top of the NFC technology and its support to integrate with your existing applications.

The platform facilitates

- Ability to join with prevailing Loyalty programs
- It is fully managed Loyalty card program including
  - Member management
  - Partner management
  - Loyalty point scheme
  - Redemption Process
- Alerts and notifications are possible via mobiles one to one member interaction

Other Features:

- Centralized management
- Different types of alerts and notifications for customers and administrators
- Tracking of customer activities
- Keeping records of Loyalty programs
- Real time monitoring

Benefits:

It gives the ability to connect with NFC technology based Loyalty programs.

It gives the vendor the chance of gathering the intellectual knowledge about the customer:

- Recognize customer preferences
- Recognize customer response to given offers
- Group Customer segmentation
- Identify lifestyle patterns of customers
- Develop behaviors profile of customers
- As a result, increase the store of goods in high demand

Allows the merchants to analyze customer transaction data

- How they shop
- How often they shop
- How much they spend at a time
- How much per month
- Preferred outlet
- Preferred benefit of shopping

### 3.7.3 Implementation in Millennium Information Technologies

MIT is one of the leading information technology solution provider in Sri Lanka which provides ICT Solutions for financial and telecommunication industry mainly. It also provides consultancy services and Information technology infrastructure to necessary institutions / Organizations.

MIT was started in 1996 in Colombo and in October 2009 it was acquired by London Stock Exchange group.

MIT is one of the first companies in Sri Lanka to use NFC application solutions. Millennium T-Gate, their main product is a reliable transaction manager which links despair NFC enabled terminals and enterprise software applications.

This entrepreneur- independent platform allows the companies to join and market goods and services of each other's to share customers using a single smart card or mobile equipment.

#### 3.7.3.1 Potential applications with MIT

Multi-function employee ID/access/voucher cards linked to GPS, databases, etc.

Privilege cards, after sales contact cards, E-Coupons which comes with mobiles and location-specific advertising for the retail and marketing sector.

Airline cards for Privilege members, Application based boarding pass and baggage handling cards, and NFC-based access control systems for the airline industry.

Personal identification cards linked to centralized patient databases for the healthcare industry.

Tracking cards with GPS and other technologies and skills-based production-line management solutions for primary producers, manufacturers, distributors, etc.

Benefit cards for employees such as Fuel through employee quotas, smart cards, etc.  
E-boarding pass and travel cash cards, season tickets for the transport industry.

## Chapter 4 – Design of Solution

This researcher wishes to use this as a base model to understand the Key contributing factors for the governance model in Sri Lankan context.

Listed below are the factors that are identified as key contributors for the governance model.

1. Master Key Management
2. Key distribution
3. NFC Readers Standardization / Life Cycle Management
4. NFC Chipset Standardization / Life Cycle Management
5. Security aspect of NFC Chips
6. Mobile Operator Security
7. Service Provisioning
8. Interoperability vulnerabilities in hardware and platforms
9. Collaboration Among Players
10. Application Design Quality
11. Service Provider Management
12. Merchants management
13. Customer Authentication Security
14. Adjusting Service Provider Conflict

These factors are categorized under governance model which was discussed previously. Factors are contributing in various capacities in NFC Eco system, but all these factors are some way or other influence the NFC Governance.

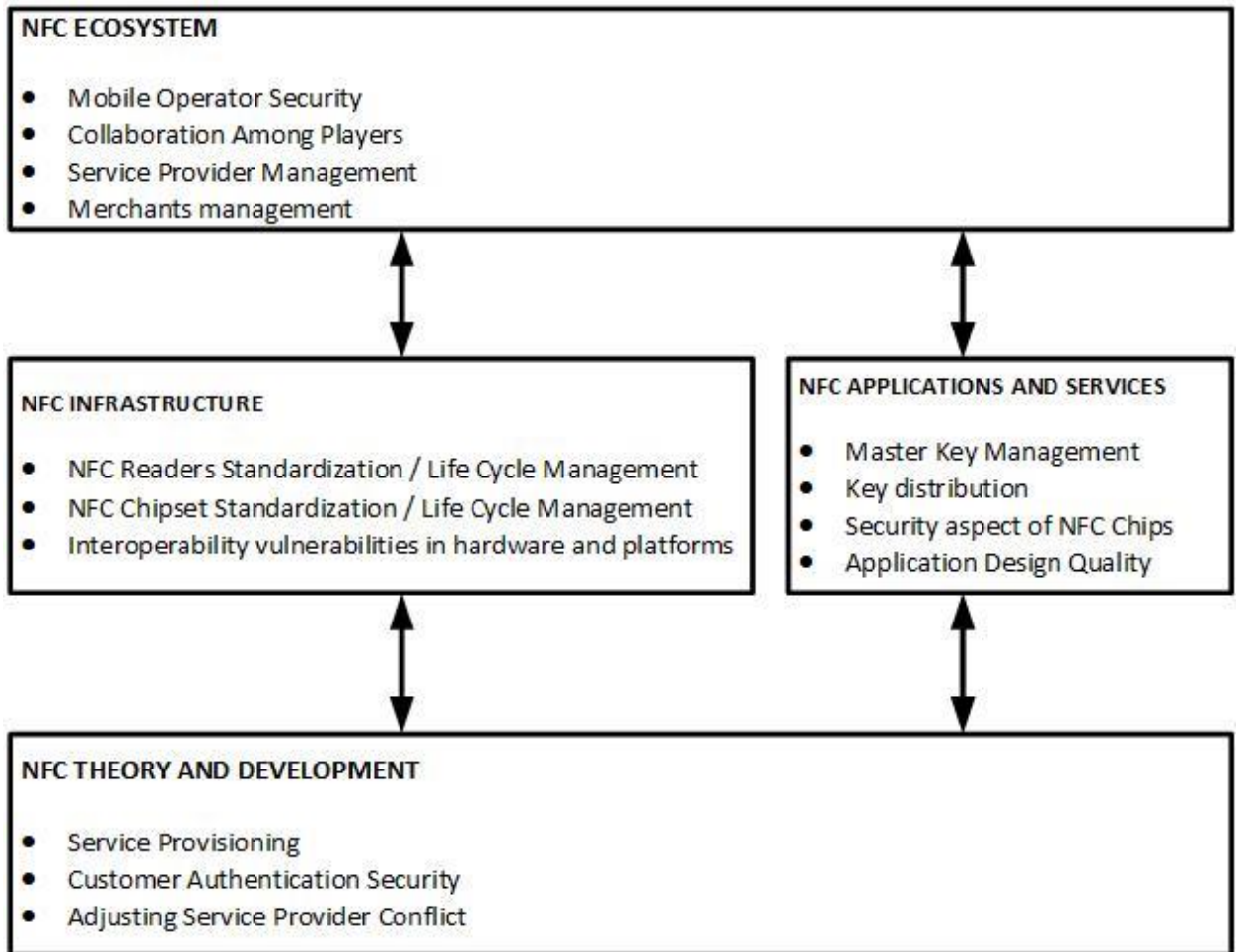


Figure 4 : Proposed Governance Model for NFC

*Figure 4.1: Proposed NFC Governance Model - Level I*

## 4.1 Proposed Governance Framework

This is the nutshell of the proposed model which covers all total span of NFC ECO System.

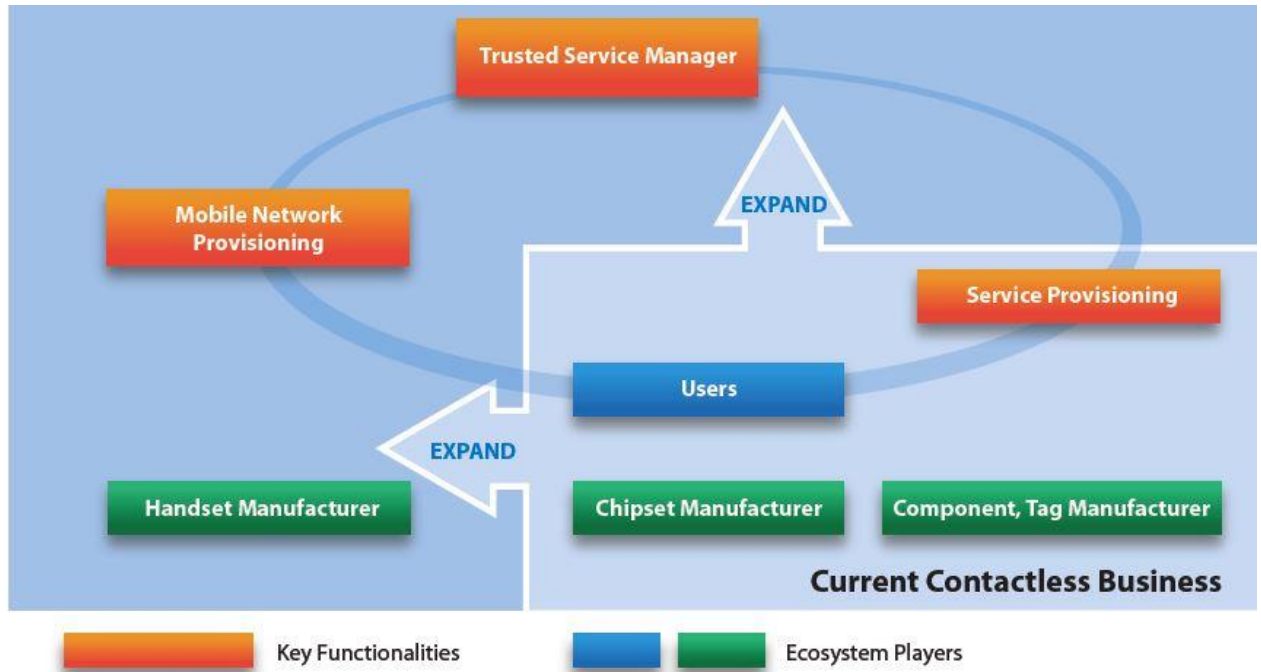


Figure 4.2: Contactless NFC Model

This is called a contactless model as we can fully automate the services from here. This Governance model is built around the Contactless Model. This model consists of Functional and none functional players and both integrated into a single platform.

It will be briefly touched upon and later in my governance frame work, this will be discussed in detail.



## 4.2 Key Functionalities in Contactless Model

### 4.2.1 Service Provisioning

Service Provisioning is the function where the users will be subscribed into new services and commission the services. This will also be tightly integrated with CRM module where the user right management will handle. In current context, this will be the point where the user will issue a contactless card. Different service providers will be subscribed into this service provisioning module and consume the service simultaneously.

### 4.2.2 Trusted Service Manager

Trusted service manager function is more important in Payment handling process where it manages the back-end function more secure for the customer. TSM is an intelligent agent who can talk to multiple APIs from different banks as well as manage the security within. It is a security in build to make sure the security is leverage since the sensitive personal data such as credit card details are managed with in TSM.

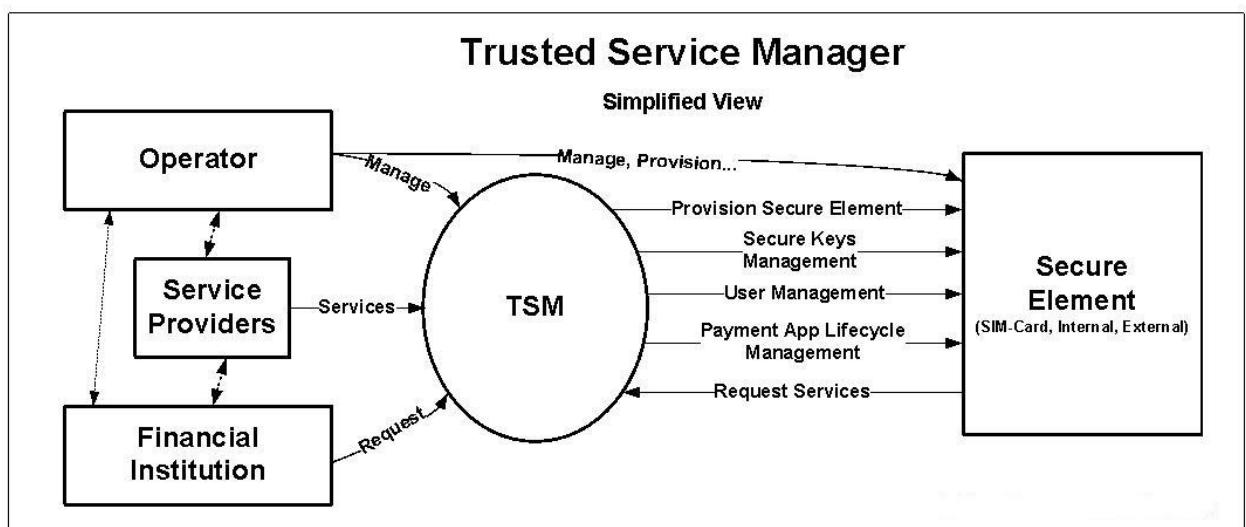


Figure 4.3: Trusted Service Manager

### 4.2.3 Mobile Network Provisioning / Security

This means adding new functionality to the existing ECO System while running the existing user services. This will maintain the existing infrastructure as it is.

### 4.2.4 Chipset Manufactures

Chipset manufacture should provide the NFC chip set which is needed for NFC devices according to the PCI Standards.

#### 4.2.5 NFC Tag Manufacturer

In fierce competition with the Mobile phone which now comes in build NFC capabilities. So, the new tags need to be state of art and combination of attractive design and price. State of the art phone comes into the market as well as cutting edge technology advancement in the phone industry will force the tag manufacturers to be vigilant.

#### 4.2.6 Service Providers

One of the key success factors for service providers is the ability to provision more services to NFC domain which can add value to the users. It is the time to rethink the strategy how the services can be marketed. Users are more driven towards the personalization and they need more personal experience in market space.

## Chapter 5 – Implementation

### 5.1 Overview

Under this section, the Governance model that is supposed to propose after going through the industry best practices will be discussed. There are some changes to be accommodated to the initial design as per the feedback received from the industry experts and the neutral observatory. This model is not yet implemented in Sri Lanka and has no plan to implement also.

#### Key Highlights of proposed model

- Mobile module is proposed to handle the multi factor authentication. This will be part and parcel of the NFC ECO System so this cannot be decoupled.
- With the technology advancement, we can bring the eye contact, Finger Scanning with mobile as second factor rather than token based validation.
- Proposed Mobile based NFC ECO System rather than a card based system. This will eliminate the additional burden on NFC cards and card life cycle management. As all the smart phones are coming in build with NFC smart tags, this can be easily implemented.
- Customer Relationship Management (CRM) Module to do the service provisioning self-portal. The operation can be handed over to None Technical Staff (Like Call Center) to manage or can be given to self-provision and self-subscribe to the services that you deem necessary.
- Data Analytic can be built on top of this layer to fraud detection, Pattern analysis, Personal payment behavior analysis

## 5.2 Evaluate the Feedback

As stated above, this model was derived based the feedback taken from the industry experts. In the context of feedback evaluation, Interview method was used since the number of experts available in Sri Lanka is lesser. Total of 10 Industry experts were interviewed and their feedback was categorized in to five main categories namely NFC Eco system, Infrastructure, Security, Data Analytics and Provisioning.

Based on their feedback, key factors that influence the governance model is derived.

Multifactor Authentication is very strongly recommended by the technology specialist and it was a key finding from the interview that was carried out.

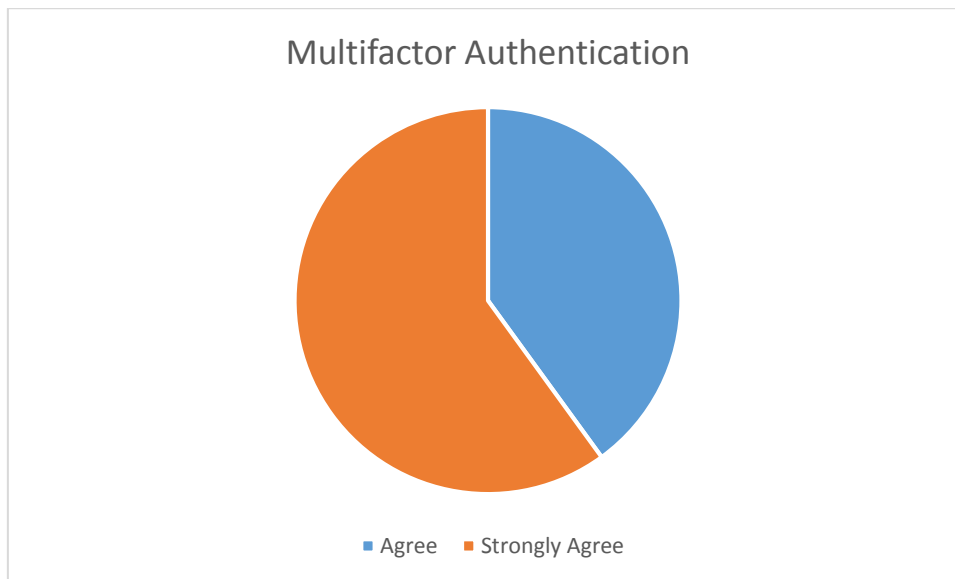


Figure 5.1: Multifactor Authentication Survey Results

From the selected experts, lot of them are vouching for soft token instead of hardware token. This is the same the researcher found from the Literature. Trend now is towards the soft token as hard token is in the decline trend.

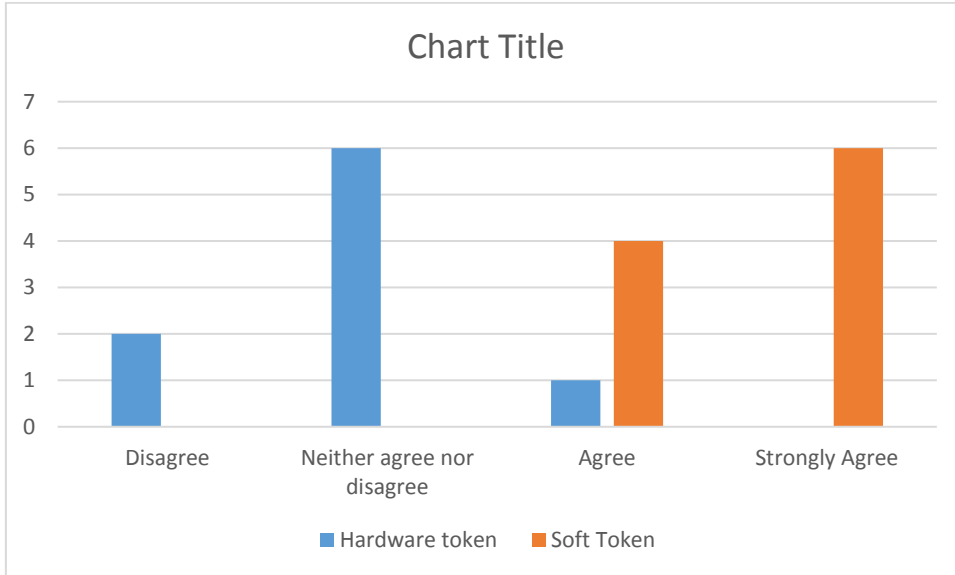


Figure 5.2: Hardware Token Vs Soft Token

Researcher has taken the cultural aspect as factor since it was found out in literature. But with the interviewed with the experts, it was proven that it's not a barrier for technology implementation.

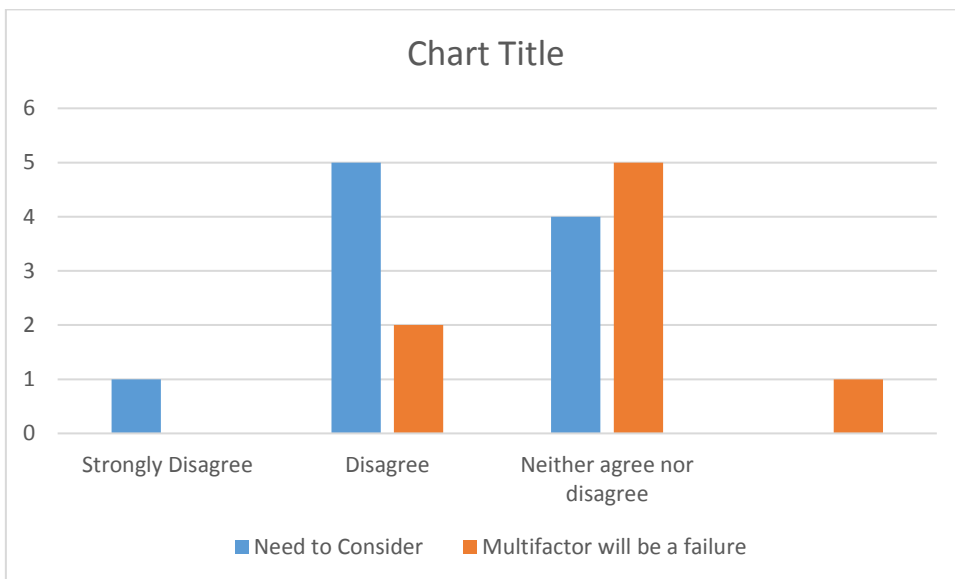


Figure 5.3: Cultural Aspect

### 5.3 Conceptual Design

Under this conceptual design, the researcher suggests the above proposed changes to the initial design. This will be an enhancement to the initial proposed model. This was validated by the industry experts from Millennium Information Technology, Dialog Axita & Mobitel Sri Lanka as stated in previous chapter.

Still this is a conceptual model which needs to implement as none of the entities mentioned above are yet to implement or plan to implement.

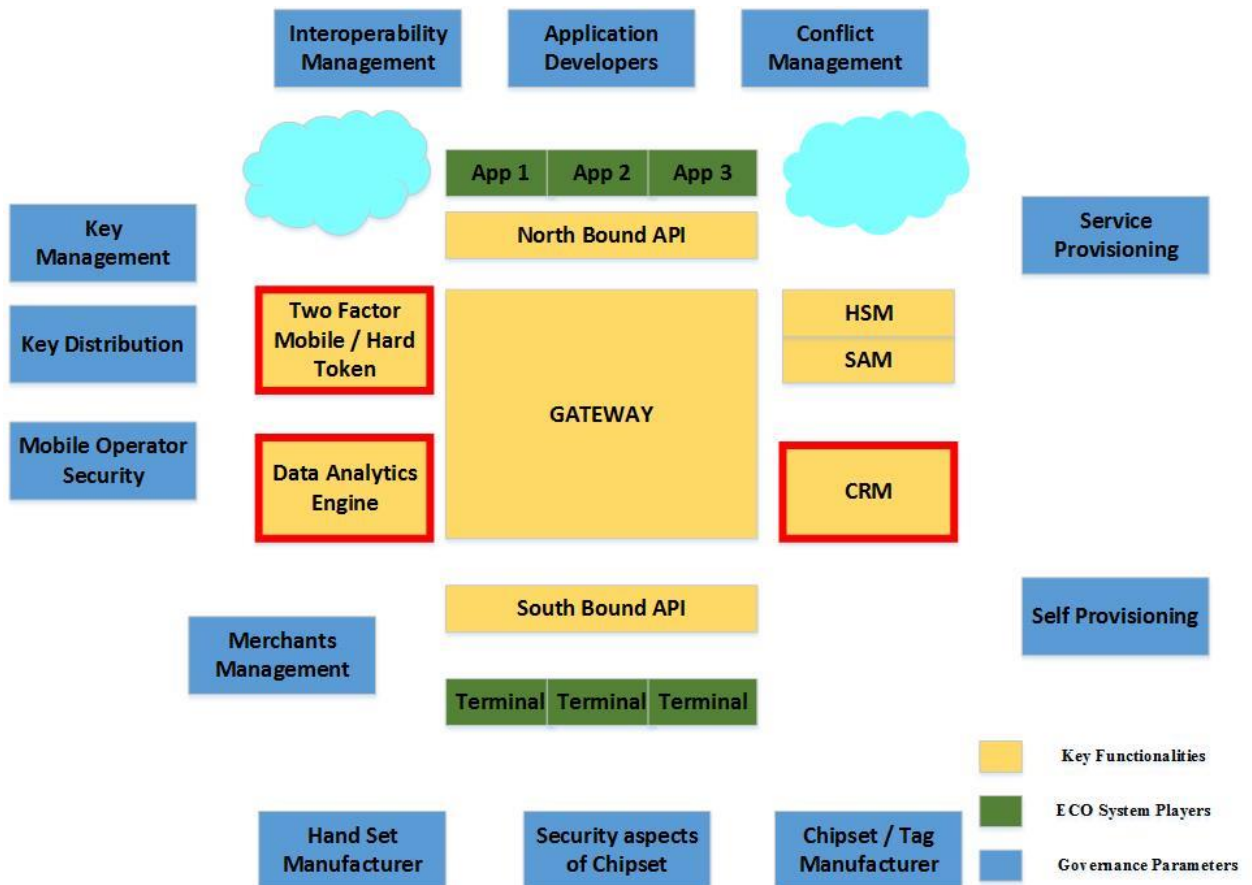


Figure 5.4: Proposed NFC Governance Model - Final

All the key contributors that were validated by the industry experts as well as endorsed my Research Literature are included. This is the first design which included the two factor Authentication into design.

## 5.3 Features in Futuristic model

### 5.3.1 Inbuilt Multifactor Authentication

The weakest link in previous models is authentication security which was not considered. With the advancement of the technology, the researcher proposes Mobile Multifactor module which talk to gateway directly. Since most of the smart phone devises are coming inbuilt with NFC technology, we might not require NFC tags which can leave out an additional burden. As the multifactor is part and parcel of the solution, this cannot be eliminated. But should leave it for the customers to pick and choose for none financial applications.

### 5.3.2 Customer Relationship Manager

All the provisioning of services is carried out by CRM. This should be a portal that can be given self-provisioning capability. Then the consumer can provision his / her own desired application. This can be granted to Merchants to self-enroll their applications to the system only if they follow the governance frame work and satisfy the requirements. Granting the permission to the users, Manage the credit limits, Enroll the users to the applications are the main features available in the CRM. This can be managed by the consumer as well as the call center agent.

### 5.3.3 Data Analytics Engine

This will be the nerve center of the NFC Domain. This will capture the data and it is available for data scientist to explore. Since this has almost all the details that we can understand the consumer, these details need to be protected. Government organizations should have the control of this data otherwise this can be used for marketing purposes.

These are the level of detail that we need to explore with IOT Platform

- How they shop
- How often they shop
- How much they spend at a time
- How much per month
- Preferred outlets
- Preferred benefit of shopping

### 5.3.4 Multifactor Authentication Application

The purpose of this application is to have an interface to register users first hand. Once the user gets registered with the application, the user will be automatically picking from next logging. The user needs to validate himself by proving the authentication code provided by Google Authenticator. This is a session key that expires every 60 seconds. So, the man in the middle attack is not possible or the probability of such attack is very low.

Application is developed using PHP Object Oriented Design concept and the backend database is MySQL. Also, used Bootstrap which is very popular for developing responsive, mobile first light weight application and the frame work is supportive of HTML, CSS & JS. Also, this research has used JQuery libraries to integrate certain security functions in this program.

Application is carrying two main components.

Mobile App (To validate the Google Multifactor Authentication)

Custom Application to register the users and validate the pin number with Google Application

#### 5.3.4.1 Logging Screen

This is the landing page of this application where users get registered at first hand on the logging interface

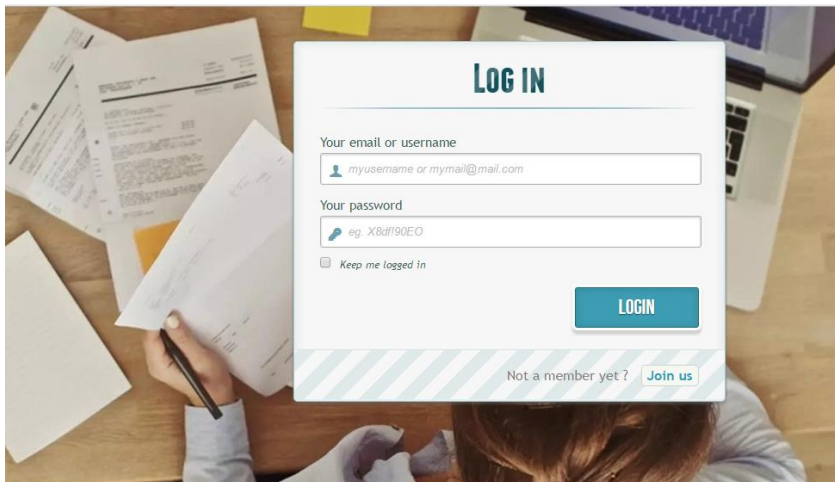


Figure 5.5: Logging Screen

For the new users, it facilitates the users to get registered with valid user name and a password just clicking the Join Us.



### 5.3.4.2 Sign up Screen

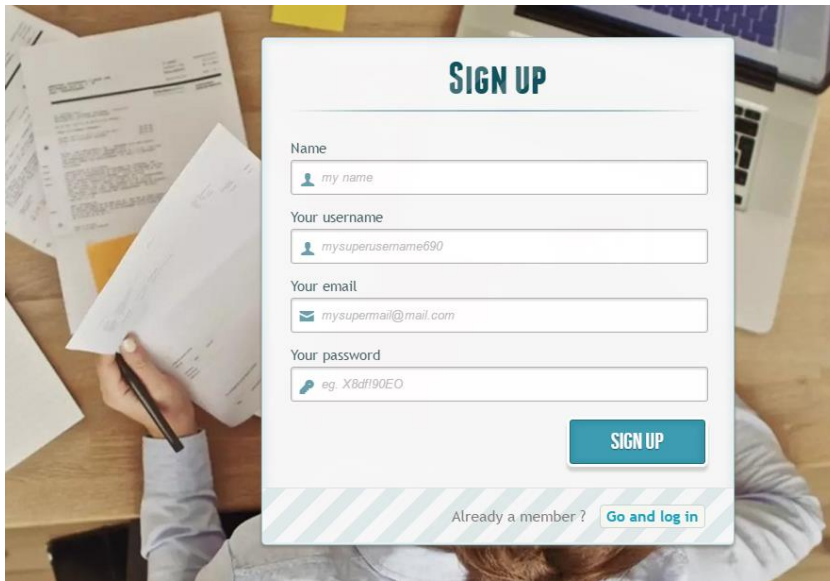
A screenshot of a 'SIGN UP' form overlaid on a background of a person working at a desk. The form has a white background with a teal header. It contains four input fields: 'Name' with the placeholder 'my name', 'Your username' with 'mysuperusername690', 'Your email' with 'mysupermail@mail.com', and 'Your password' with 'eg. X8df!90EO'. A teal 'SIGN UP' button is at the bottom right. Below the button, there is a link 'Already a member? Go and log in'.

Figure 5.6: Sign Up Screen

### 5.3.4.3 Multifactor Handling Screen

Once the user account is created, you are asked to validate the user with Google Authentication application code generated from your phone.

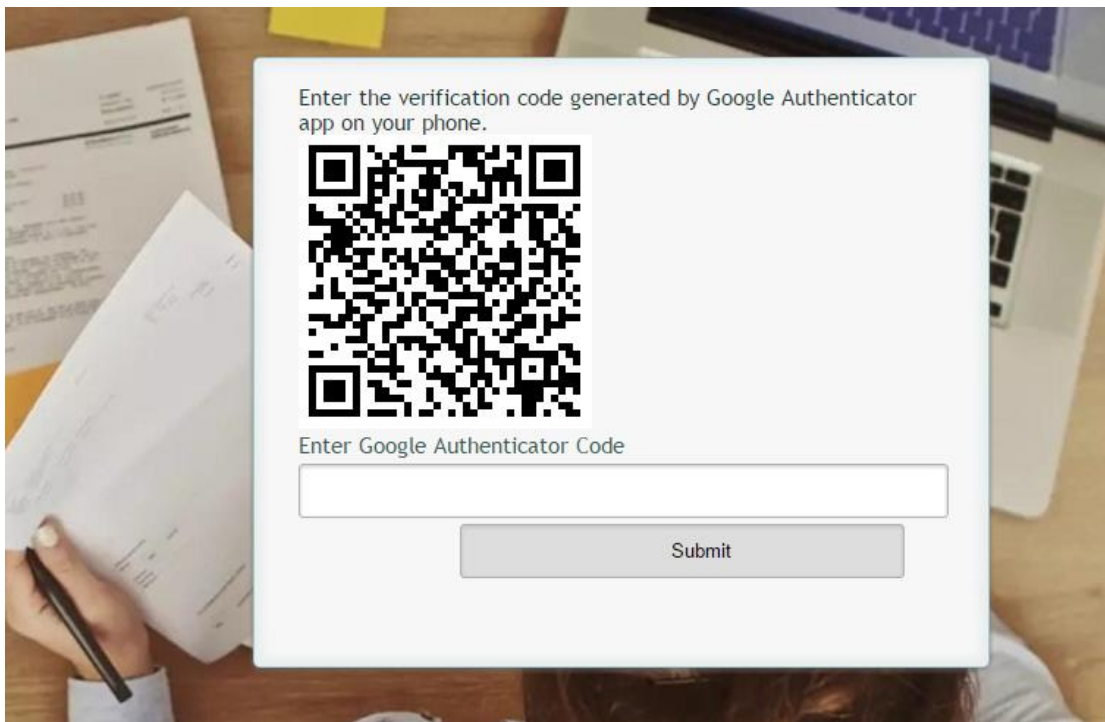
A screenshot of a 'Validate' screen overlaid on the same background as Figure 5.6. The screen has a white background with a teal header. It contains the text 'Enter the verification code generated by Google Authenticator app on your phone.' followed by a large QR code. Below the QR code is the text 'Enter Google Authenticator Code' and a white input field. At the bottom is a grey 'Submit' button.

Figure 5.7: Validate Screen

Once the Google Authentication Code generated from the app in your phonies provided, you are authenticated with the user name.

After your reach authentication, you are required to provide the random generated google authenticator code as your second factor for authentication.

The google Authenticator code is refreshed by every 60 second so the chances of manipulating the result are very little.

#### 5.3.4.4 Welcome User Screen

Once you provide with the code, you will be authenticated

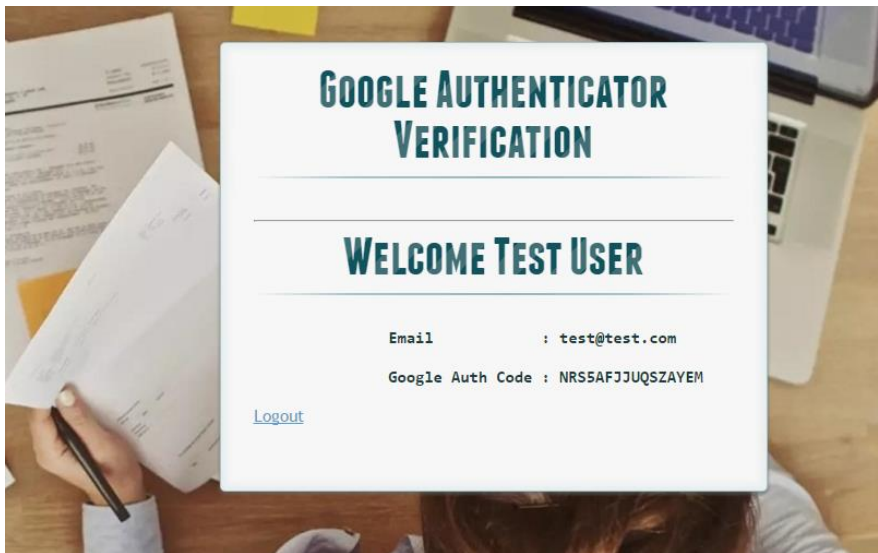


Figure 5.8: Authentication Screen

Only successful credentials will be validated and others will be directed to an error handling page.

### 5.3.4.5 Program Code in Nutshell

CSS Style Sheet is used to make the application more user friendly.

```
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en" class="no-js"> <!--
```

Figure 5.9: CSS Style Sheet

To make the pages more attractive certain CSS Style sheets were used.

This is where it is pointed to the database Username, Password, base URL and database name. Furthermore, database Connection variable use to create connection is also mention here.

```

<?php
session_start();
/* DATABASE CONFIGURATION */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'root');
define('DB_PASSWORD', '');
define('DB_DATABASE', 'gauth');
define("BASE_URL", "http://localhost/php/");

function getDB()
{
    $dbhost=DB_SERVER;
    $dbuser=DB_USERNAME;
    $dbpass=DB_PASSWORD;
    $dbname=DB_DATABASE;
    try {
        $dbConnection = new PDO("mysql:host=$dbhost;dbname=$dbname", $dbuser, $dbpass);
        $dbConnection->exec("set names utf8");
        $dbConnection->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
        return $dbConnection;
    }
    catch (PDOException $e) {
        echo 'Connection failed: ' . $e->getMessage();
    }
}

```

Figure 5.10: Configuration File

In the index page, it includes config.php

This captures the current user who has logged in.

```

include('class/userClass.php');
$userClass = new userClass();

```

Figure 5.11: Current User

User google Authentication ID is created by the below code.

```
require_once 'googleLib/GoogleAuthenticator.php';
$ga = new GoogleAuthenticator();
$secret = $ga->createSecret();
```

Figure 5.12: Google Authentication

Under the Index page HTML, view was added two forms to capture logging and registration details.

```
<div id="register" class="animate form">
  <form method="post" action="" name="signup">
    <h1> Sign up </h1>
    <p>
      <label for="username signup" class="uname" data-icon="u">Name</label>
      <input id="username signup" name="nameReg" required="required" type="text" placeholder="my name" />
    </p>
    <p>
      <label for="username signup" class="uname" data-icon="u">Your username</label>
      <input id="username signup" name="usernameReg" required="required" type="text" placeholder="mysuperusername690" />
    </p>
    <p>
      <label for="email signup" class="youmail" data-icon="e" > Your email</label>
      <input id="email signup" name="emailReg" required="required" type="email" placeholder="mysupermail@mail.com"/>
    </p>
    <p>
      <label for="password signup" class="youpasswd" data-icon="p">Your password </label>
      <input id="password signup" name="passwordReg" required="required" type="password" placeholder="eg. X8df!90E0"/>
    </p>
    <p class="signin button">
      <input type="submit" value="Sign up" name="signupSubmit"/>
    </p>
    <p class="change_link">
      Already a member ?
      <a href="#tologin" class="to_register"> Go and log in </a>
    </p>
  </form>
</div>
```

Figure 5.13: Registration Detail

In this screen, you are required to provide a valid user name and password and this will carry your authenticity for the application.

In Click Event of the Submit button, following code set is executed.

```

if (!empty($_POST['signupSubmit'])) {
    $username = $_POST['usernameReg'];
    $email = $_POST['emailReg'];
    $password = $_POST['passwordReg'];
    $name = $_POST['nameReg'];
    $username_check = preg_match('~^[A-Za-z0-9_]{3,20}$~i', $username);
    $email_check = preg_match('~^[a-zA-Z0-9._-]+@[a-zA-Z0-9._-]+\.[a-zA-Z]{2,4}$~i', $email);
    $password_check = preg_match('~^[A-Za-z0-9!@#%&*()_]{6,20}$~i', $password);

    if ($username_check && $email_check && $password_check && strlen(trim($name)) > 0) {
        $uid = $userClass->userRegistration($username, $password, $email, $name, $secret);
        if ($uid) {
            $url = BASE_URL . 'device_confirmations.php';
            header("Location: $url");
        } else {
            $errorMsgReg = "Username or Email already exists.";
        }
    } else {
        $errorMsgReg = "Enter valid details.";
    }
}
}

```

Figure 5.14: Validate User

In this code execution, it checks the user name, e-mail address and password. It checks the validity of the values entered and calls the User class to pass the values to the database and saves it.

Afterwards it creates a UID only if the UID does not exist in the DB and redirect the page to device confirmation. It includes the QR Code to scan from the device. If the username or e-mail id already exists in the database, then an error message will pop to inform that the user already exists.

UID created is associated with user name and e-mail address.

## User Logging form

In the user logging form, below code is executing.

```
<div id="login" class="animate form">
  <form method="post" action="" name="login">
    <h1>Log in</h1>
    <p>
      <label for="username" class="uname" data-icon="u" > Your email or username </label>
      <input id="username" name="usernameEmail" required="required" type="text" placeholder="myusername or mymail@mail.com"/>
    </p>
    <p>
      <label for="password" class="youpasswd" data-icon="p"> Your password </label>
      <input id="password" name="password" required="required" type="password" placeholder="eg. X8df!90E0" />
    </p>
    <p class="keeplogin">
      <input type="checkbox" name="loginkeeping" id="loginkeeping" value="loginkeeping" />
      <label for="loginkeeping">Keep me logged in</label>
    </p>
    <p class="login button">
      <input type="submit" value="Login" name="loginSubmit" />
    </p>
    <p class="change_link">
      Not a member yet ?
      <a href="#toregister" class="to_register">Join us</a>
    </p>
  </form>
</div>
```

Figure 5.15: User Logged In

Click login Submit go to login function and check the user name, whether the email is correct and if it is correct it will send the device confirmation.php it includes QR code to scan. Otherwise it sends an error message.

```
if (!empty($_POST['loginSubmit'])) {
  $usernameEmail = $_POST['usernameEmail'];
  $password = $_POST['password'];
  if (strlen(trim($usernameEmail)) > 1 && strlen(trim($password)) > 1) {
    $suid = $userClass->userLogin($usernameEmail, $password, $secret);
    if ($suid) {
      $url = BASE_URL . 'device_confirmations.php';
      header("Location: $url");
    } else {
      $errorMsgLogin = "Please check login details.";
    }
  }
}
```

Figure 5.16: Handling User Logging

## Devise Confirmation.php

This includes QR code enter form and when user login or register takes user details through user class like following.

```
include('class/userClass.php');
$userClass = new userClass();
$userDetails = $userClass->userDetails($_SESSION['uid']);
$secret = $userDetails->google_auth_code;
$email = $userDetails->email;
```

Figure 5.17: QR Code

Afterwards take the e-mail address and validate with the QR code like below

```
require_once 'googleLib/GoogleAuthenticator.php';

$ga = new GoogleAuthenticator();

$qrcodeUrl = $ga->getQRCodeGoogleUrl($email, $secret, 'Auth_app');
```

Figure 5.18: QR Code Validation

Below code will added qrCodeUrl image and form to enter google code appear in mobile app.

```
<div id="img">
  <img src='<?php echo $qrcodeUrl; ?>' />
</div>

<form method="post" action="home.php">
  <label>Enter Google Authenticator Code</label>
  <input type="text" class="form-control" name="code" />
  <input type="submit" class="btn btn-info" style="width:60%;margin-left:25%;"/>
</form>
```

Figure 5.19: Validate with App



Home.php

When Submit, form go to home.php page it shows user details.

Include user details and google id and it takes using following code segment.

```
include('config.php');
include('class/userClass.php');
$userClass = new userClass();
$userDetails = $userClass->userDetails($_SESSION['uid']);

if ($_POST['code']) {
    $code = $_POST['code'];
    $secret = $userDetails->google_auth_code;
    require_once 'googleLib/GoogleAuthenticator.php';
    $ga = new GoogleAuthenticator();
    $checkResult = $ga->verifyCode($secret, $code, 2); // 2 = 2*30sec clock tolerance

    if ($checkResult) {
        $_SESSION['googleCode'] = $code;
    } else {
        echo 'FAILED';
    }
}
```

Figure 5.20: QR Code Change Sequence Code

User details html view shows following code segment.

```
<h1>Welcome <?php echo $userDetails->name; ?></h1>

<pre>
<b> Email           : <?php echo $userDetails->email; ?></b><br>
<b> Google Auth Code : <?php echo $userDetails->google_auth_code; ?></b>
</pre>
<h4><a href="<?php echo BASE_URL; ?>logout.php">Logout</a></h4>
```

Figure 5.21: User Logout

When click, logout go to logout.php and clear session UID and go to index page.

## Userclass.php

This class includes user registration, user login and user details functions.

User registration function.

```

/* User Registration */
public function userRegistration($username,$password,$email,$name,$secret)
{
    try{
        $db = getDB();
        $st = $db->prepare("SELECT uid FROM users WHERE username=:username OR email=:email");
        $st->bindParam("username", $username,PDO::PARAM_STR);
        $st->bindParam("email", $email,PDO::PARAM_STR);
        $st->execute();
        $count=$st->rowCount();
        if($count<1)
        {
            $stmt = $db->prepare("INSERT INTO users(username,password,email,name,google_auth_code)");
            $stmt->bindParam("username", $username,PDO::PARAM_STR) ;
            $hash_password= md5($password);
            $stmt->bindParam("hash_password", $hash_password,PDO::PARAM_STR) ;
            $stmt->bindParam("email", $email,PDO::PARAM_STR) ;
            $stmt->bindParam("name", $name,PDO::PARAM_STR) ;
            $stmt->bindParam("google_auth_code", $secret,PDO::PARAM_STR) ;
            $stmt->execute();
            $uid=$db->lastInsertId();
            $db = null;
            $_SESSION['uid']=$uid;
            return true;
        }
    }
    else
    {
        $db = null;
        return false;
    }
}

```

Figure 5.22: User Class

## User Login Function

```
/* User Login */
public function userLogin($usernameEmail,$password,$secret)
{
    $db = getDB();
    $hash_password= md5($password);
    $stmt = $db->prepare("SELECT uid FROM users WHERE (username=:usernameEmail
    $stmt->bindParam("usernameEmail", $usernameEmail,PDO::PARAM_STR) ;
    $stmt->bindParam("hash_password", $hash_password,PDO::PARAM_STR) ;
    $stmt->execute();
    $count=$stmt->rowCount();
    $data=$stmt->fetch(PDO::FETCH_OBJ);
    $db = null;
    if($count)
    {
        $_SESSION['uid']=$data->uid;
        $_SESSION['google_auth_code']=$google_auth_code;
        return true;
    }
    else
    {
        return false;
    }
}
```

Figure 5.23: User Logging Function

## 5.4 Testing of the Application

### Test Cases

Several test cases were carried out to validate the User Authentication module.

1. Create a duplicate e-mail and validate the user

TC#	Test Case	Expected Results	Actual Results	Pass / Fail
1	Try to register a new user under already registered E-mail address	Error message should pop up saying "E-mail already exist"		PASS

Approach: Try to create a new user from the user already exist

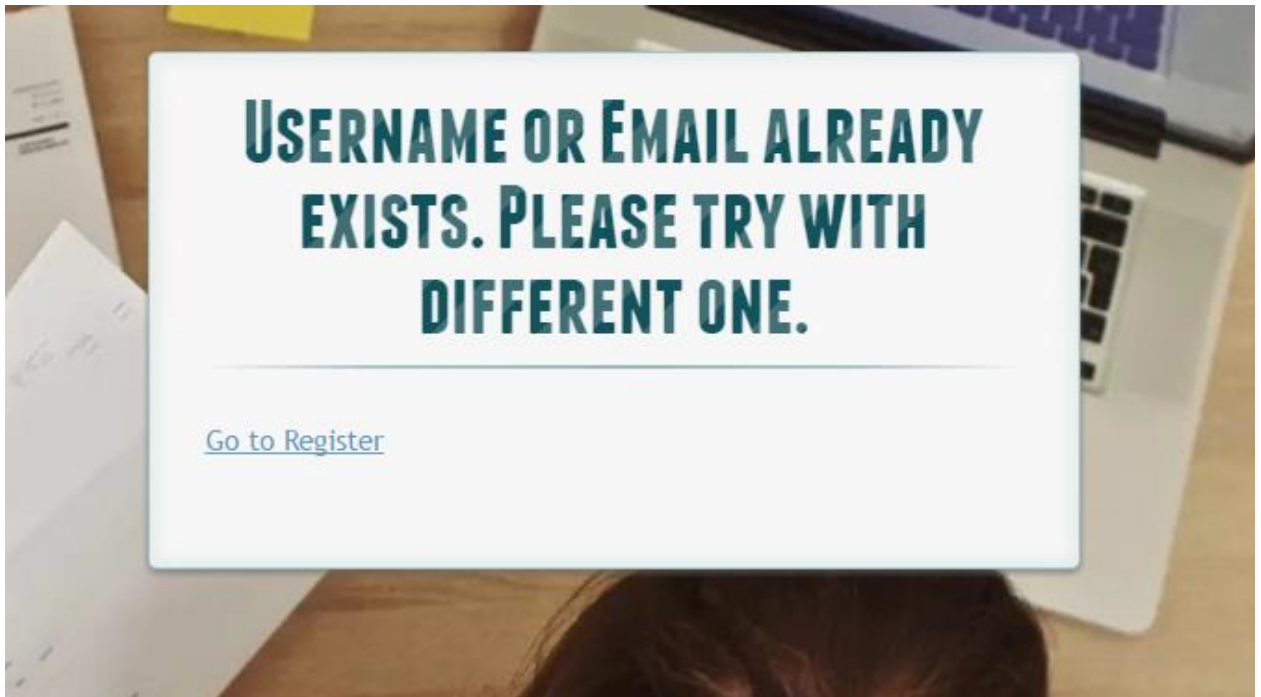


Figure 5.24: User E-mail Check

Result: Error message will pop up saying the "User already exists"

## 2. Try to duplicate the user name

TC#	Test Case	Expected Results	Actual Results	Pass / Fail
2	Try to register a new user under already exist user name	Error message should pop up saying "User name already exist"		PASS

Approach: Try to create a new user with already exist user name

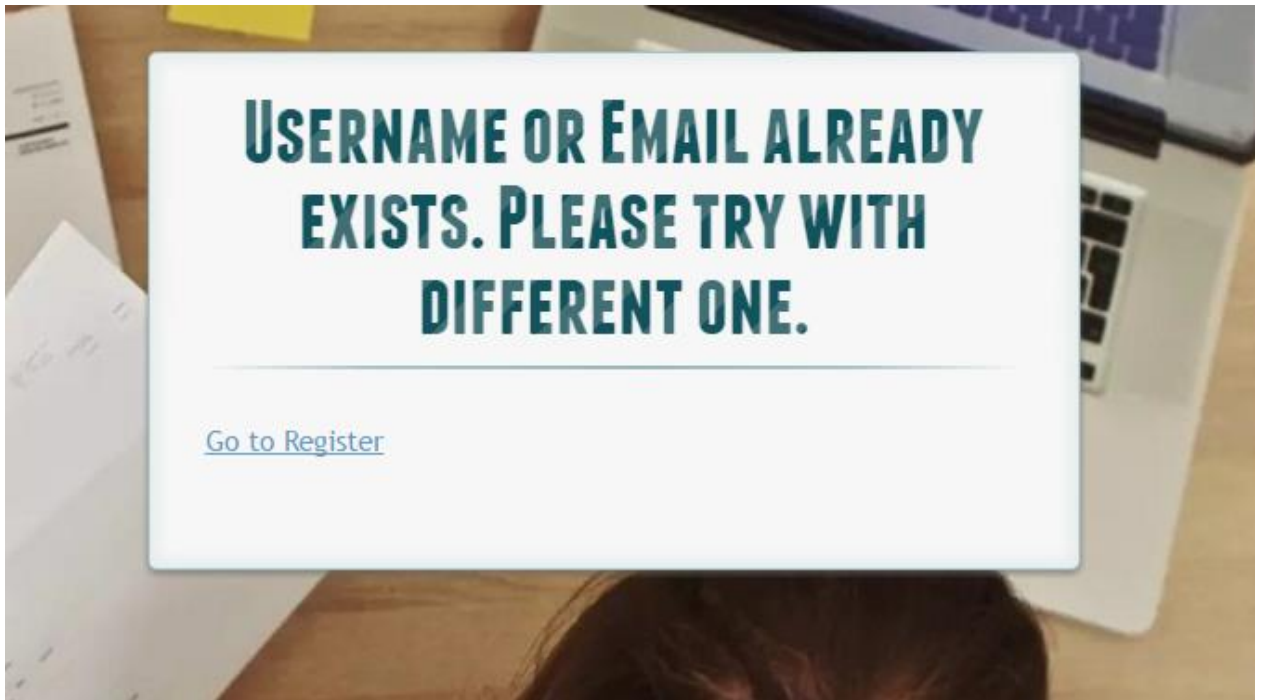


Figure 5.25: User Name Check

Result: Same as previous test case, error message will pop up saying "User already exists"

## 3. Three unsuccessful user logging attempts

TC#	Test Case	Expected Results	Actual Results	Pass / Fail
3	Try to be logging using a user name where password is not matching	After 3 attempts, user should be locked out		PASS

Approach: Try 3 unsuccessful logging attempts with wrong password

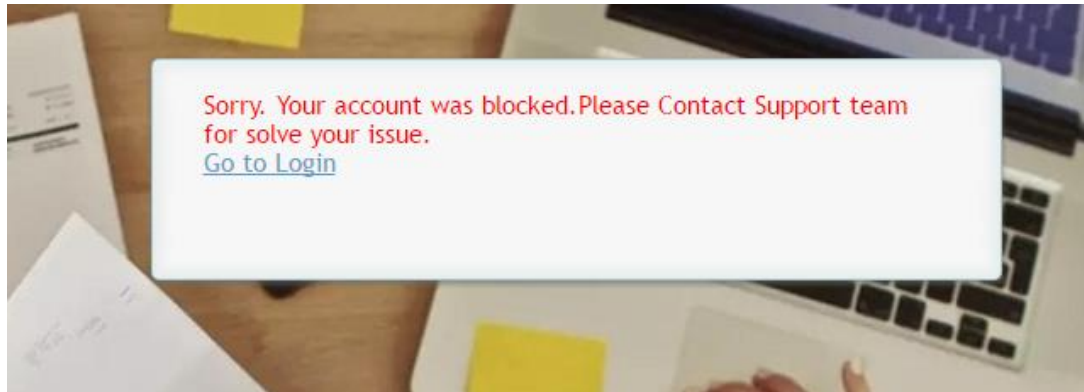


Figure 5.26: User Blocked

## 4. Providing wrong QR Code for authentication

TC#	Test Case	Expected Results	Actual Results	Pass / Fail
4	Try to put a wrong QR code	If the QR Code is wrong, then user should lock out		PASS

Approach: Insert wrong QR Code to validate

## 5. Understand the user logging devise

TC#	Test Case	Expected Results	Actual Results	Pass / Fail
5	Try to be logging using a new devise	After 3 attempts, user should be locked out		PASS

Approach: Register the devise (Apple, Android, Windows, etc..) in the first logging and not allow other devises

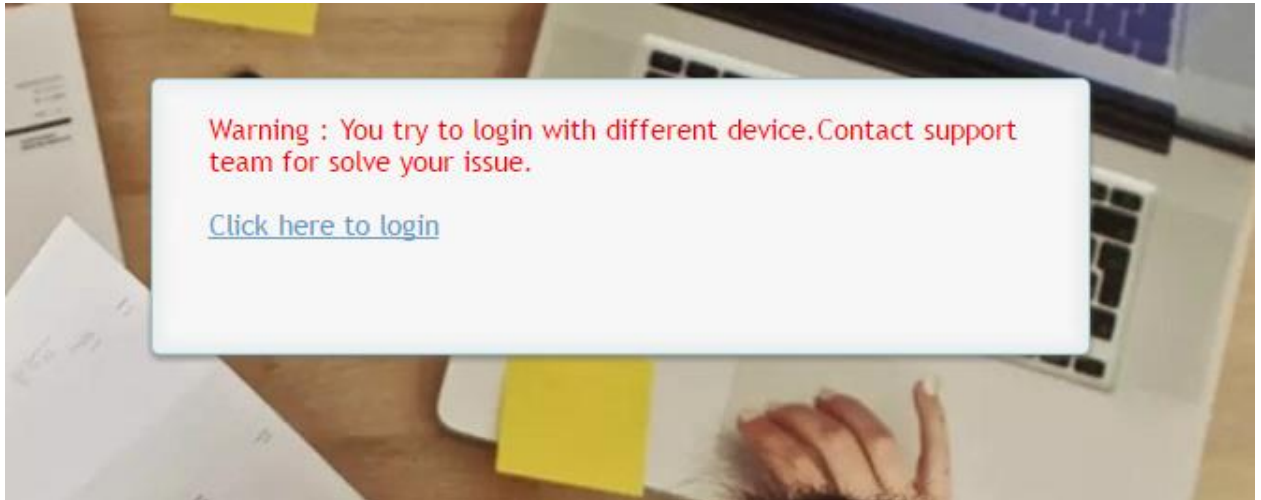


Figure 5.27: Devise Validate

## Chapter 6 – Conclusion and Future Work

### 6.1 Introduction

In this chapter, summarizing is done and understanding for recommendation and what is left for future researchers to mind is discussed. In the field of Near Field Communication in the world context, it has evolved a lot around smart phone technology. Lot of services are in the offering in many diversified areas. Lot of services are yet to implement in Sri Lanka as technology embrace is very slow in this part of the world. There are handful of services offer in Sri Lanka in this space but with lot of restrictions. Sometimes the offering is limiting to none value added services. In the corporate world, there's a big demand for paperless automations as well as moneyless transactions. Some applications such as fuel cards are in use by few corporates but majority is still working in traditional way.

### 6.2 NFC Governance Framework

NFC is a booming technology in Sri Lankan context and lot of work has been done by many organizations in Sri Lanka. Yet the technology is still premature compared to other real world examples. NFC application and its ECO System are still limited to very primitive applications like Fuel cards, Meal Management Solutions. Certain initiatives are taken to bring this to the next level such as ticketing solution for Public Transportation yet the technology acceptance is very low in Sri Lanka. There is not much enthusiasm in general public to embrace the new technologies to make their life easy as traditional paper based work is still the dominant work flow in Sri Lanka.

Recommendation can be categorized into three sections which need to address separately. Strategies should plan accordingly to these three main sections.

#### 6.2.1. User Recommendation

- Need to have mindset change to accept the technology instead of paper based work flow.
- Should accept One Card Many service concept and adhere to the technology road map.

#### 6.2.2 Technology Provider Recommendation

- All the NFC development communities should team up and come up with a single model to which everyone can contribute and accept.
- Accept the Governance model proposed in previous chapter which includes security, availability and reliability.
- Encourage Interoperability between providers.
- Not to use proprietary protocol and agreed on an open stack.
- Agreed on common standard proposed in governance model.
- Like NFC Forum, form an Alliance to take the technology forward.



### 6.2.3 Governance Body Recommendation

- Ideally this should come under Government organization like TRC.
- Motivation from government to the application developers, Merchants and end users.
- Tax benefits for all stake holder for an agreed time frame to promote the technology.
- Facilitate technological advancement.
- Facilitate tax benefits for NFC readers, Cards, NFC enable smart phone.
- Regulate the Governance Framework.
- Involvement of Government body for data analytics module as it contains personal information.

### 6.3 Multifactor Authentication Application

With the introduction of lot of applications in to NFC Platform, researcher believe the Multifactor authentication is the way forward. Since lot of financial applications are coming in to play, multifactor is must to have for way forward. Researcher is also believing with the penetration of mobile smart phones, it's not required the hard token going forward. NFC enable mobile can do the work as multifactor application can be with in mobile application pool. Researcher believe the multifactor should not limit to single product, also can be diversified based on the need. Multifactor will resolve the security concern in financial transactions as validation of the person is required. This will resolve the biggest concern in NFC ECO system as validation of the user is always a challenge. Also, this simplify the process and allow the freedom for the users to do pool proof transaction.

### 6.4 Recommendation for Future work

There are many areas needed to be touched on NFC based research in the future. In the Sri Lankan context, this is a new technology and lot of potential areas are there for further studies.

- NFC Regulation is not a very popular topic still in Sri Lanka. With the governance model introduction, I presume regulation will become a hot topic in the future.
- Card less NFC adoption is something that we might talk a lot in the future with the rise of smart phones.
- Data Analytics using NFC data is somewhat interested topic which might take little bit of time to gather the data.
- New Factors that can influence the NFC governance such as Social Media.
- Self-provisioning of NFC Services to my own tag / device.
- Financial Transaction model for NFC ECO System in Sri Lanka.

## 6.5 Limitation in Research

Since the NFC in Sri Lankan context is not a very widely used technology, it was very difficult to gather data. Data on governance model was also limited. There are only few experts in Sri Lanka who can give a view point on technology as well as governance model.

Biggest challenge was to gather NFC related data in Sri Lankan context as no such database is available in ready to refer format. Lack of enthusiasm in implementing such technology in Sri Lanka is another key drawback.

Also, the idea of multifactor is not anyone else has thought in Sri Lanka. It is good to know Information Technology Agency of Sri Lanka is interested in this idea and they are in the first level discussion to take this technology.

## 6.6 Final Conclusion

The Researcher is confident that the Governance Framework discussed in this section is very much appropriate to the Sri Lankan context. But to implement this in Sri Lanka, need to have strong governance body to drive the process. Also, the researcher is believed this can bring lot of benefits to the country as lot of applications can be put in to a single card. To Implement Multifactor authentication for authenticity, it requires certain mind changing initiatives to convince the general public. Also, the awareness of Security will do lot of good to implement this.

## Appendix

### Appendix 1

#### Interview Questionnaire to understand the factors influencing NFC Governance Model

1. What's your gender?

Male

Female

2. What's your highest Educational Qualification?

Master's Degree

General Degree

Upper School

3. What's your Job profile?

NFC Architect

NFC Application Developer

Technology Evangelist

4. How long you have been in NFC Domain in your job function?

More than 8 years

Between 5-8 years

Between 3-5 Years

Below 3 Years

5. Perceived NFC ECO System

1- Strongly Disagree

2- Disagree

3- Neither agree nor disagree

4- Agree

5- Strongly Agree

	1	2	3	4	5
Mobile Operator Security during data transmission is a key factor					
Merchants and their performance is a key factor in governance model					
Service providers such as bank are key factor in governance model					
Collaboration among merchants are key factor in governance model					

6. Perceived NFC Infrastructure

1- Strongly Disagree

2- Disagree

3- Neither agree nor disagree

4- Agree

## 5- Strongly Agree

	1	2	3	4	5
NFC reader's capabilities are key governance factor					
Manage the life cycle of readers is required					
NFC Chipset quality is a key factor in governance model					
Interoperability of the hardware is very much required					

## 7. Perceived NFC Security

- 1- Strongly Disagree
- 2- Disagree
- 3- Neither agree nor disagree
- 4- Agree
- 5- Strongly Agree

	1	2	3	4	5
Multifactor Authentication is required for application security					
Server level encryption is required for the NFC security					
Mobile Operator security is a key factor in NFC governance					
Hardware token is preferred for multi factor Security					
Soft Token is preferred for Multi factor Security					

## 8. Data Analytics using NFC data

- 1- Strongly Disagree
- 2- Disagree
- 3- Neither agree nor disagree
- 4- Agree
- 5- Strongly Agree

	1	2	3	4	5
Government organization should be the governance body since the data is sensitive					
Data Analytics is required for understand the patterns of user behaviors					

## 9. Provisioning of Services

- 1- Strongly Disagree
- 2- Disagree
- 3- Neither agree nor disagree
- 4- Agree
- 5- Strongly Agree

	1	2	3	4	5
Should be able to handle the provisioning with Call center operation					
Self-provisioning is a key factor in governance model					

## 10. Cultural Aspect of Governance

- 1- Strongly Disagree
- 2- Disagree
- 3- Neither agree nor disagree
- 4- Agree
- 5- Strongly Agree

	1	2	3	4	5
Need to consider cultural aspect before proposing a governance model					
Multi factor may not be a success with the human behavior in Sri Lanka					

## Appendix 2

## Questionnaire feedback on Governance Model

			1	2	3	4	5	6	7	8	9	10
1	Gender		1	1	1	2	1	1	1	1	1	1
2	Education		1	2	1	1	2	1	2	2	3	1
3	Job Profile		1	2	1	2	2	3	1	2	2	2
4	Experience		2	2	2	2	2	3	2	2	2	1
5	ECO System	Mobile Operator Security	4	5	4	5	4	4	5	5	5	5
		Merchants Performance	3	4	3	3	3	4	4	5	3	4
		Service Provider	4	4	4	3	4	5	5	4	4	3
		Collaboration	4	5	5	5	5	4	5	5	4	4
6	Infrastructure	NFC reader's capabilities	3	4	4	3	3	3	4	3	3	4
		Readers Life Cycle Management	4	4	4	3	5	5	5	5	3	5
		NFC Chipset quality	3	3	3	4	3	4	4	3	5	3
		Interoperability	4	4	5	4	3	4	5	4	4	5
7	Security	Multifactor Authentication	4	5	5	5	5	4	5	5	4	4
		Server level encryption	4	3	4	5	4	4	5	5	5	5
		Hardware token	3	3	2	3	4	3	3	3	2	3
		Soft Token	4	5	5	5	5	4	4	5	4	5
8	Data Analytics	Governance Body	4	5	4	4	3	3	4	3	4	3
		Data Patterns	3	4	3	3	4	3	4	3	4	4
9	Provisioning	Call Center Provisioning	3	3	4	4	3	4	5	3	3	4
		Self-Provisioning	4	3	5	4	5	4	3	4	3	4
10	Cultural Aspect	Need to Consider	3	3	2	2	3	2	2	3	1	2
		Multifactor will be a failure	3	4	3	2	2	3	3	2	2	3

## Appendix 3

### Questionnaire for multifactor Supporting Application Evaluation

1. Which category you are best suited?
  - NFC Application Developer
  - NFC Application Architect
  - NFC Application User
  
2. Are you using NFC Application in any capacity?
  - Yes
  - No
  
3. Do you convince with NFC technology?
  - Yes
  - No
  
4. Are you agreed to use second factor for Authentication?
  - Yes
  - No

#### Feedback on the application

- 1- Strongly Disagree
- 2- Disagree
- 3- Neither agree nor disagree
- 4- Agree
- 5- Strongly Agree

	1	2	3	4	5
Interfaces are very much user friendly					
Navigation of the interfaces are very smooth					
Google Authentication is convenience					
Google Authenticator is easy to use					
Authenticator is available in all market places					
Security controls in place are adequate					

## References

- [1] Sungbum Kim, Teyong Yang, Dongwook Kim “Critical Success Factors of Convergence Technology Commercialization: Near Field Communication” *IEEE Technology And Society Magazine*, 2013
- [2] Ann Cavoukian “Mobile Near Field Communication keep it Secure & Private”, *ISSA Journal*, 2013 August
- [3] J.O.Y. Pigneur, “An assessment of NFC for future mobile payment systems,” in *Proc. 6th Int. Conf, Information and Communication for Mobile Business (ICMB2007)*, 2007.
- [4] Madlmayr, G. Dillinger, O. Langer, J. and Scharinger, J. (2008), ‘Management of Multiple Cards in NFC-Devices,’ *Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications*, ISBN: 978-3-540-85892-8, 8-11 September 2008, London, UK, 149-161.
- [5] Hevner, A. R. March, S. T. Park, J. and Ram, S. (2004), ‘Design Science in Information Systems Research,’ *MIS Quarterly*, 28 (1), 75-105.
- [6] Busra OZDENIZCI, Mehmet AYDIN, Vedat COSKUN, Kerem OK, “NFC Research Framework: A Literature Review & Future Research Directions”, *IBIMA Conference*, June 2010
- [7] Muhammad Qasim Saeed, “Authentication Issues in Near Field Communication and RFID”, *University of London*, 2014
- [8] Jan Ondrus, Yves Pigneur “An Assessment of NFC for Future Mobile Payment Systems”, *University of Lausanne, Switzerland*, 2010
- [9] Jonathan Liebenau, Silvia Elaluf-Calderwood, Patrik Karrberg and Gus Hosein “Near Field Communications; Privacy, Regulation & Business Models”, *London School of Economics and Political Science*, October 2011
- [10] Henning Siitonen Kortvedt, “Securing Near Field Communication”, *Norwegian University of Science and Technology*, June 2009
- [11] <http://searchsecurity.techtarget.com/feature/The-top-multifactor-authentication-products> (Last Checked on February 22, 2017)
- [12] <https://www.abiresearch.com/market-research/product/1013359-nfc-product-trends-and-controller-market-s/>, August 19, 2015 (Last checked on January 18, 2017)
- [13] B. Benyo, A. Vilmos, K. Kovacs and L. Kutor “The Design of NFC Based Application”, *Budapest University of Technology and Economics*, April 2014
- [14] <http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-ww> (Last checked on December 18, 2016)
- [15] <http://www.smartcardalliance.org/slideshows-201200511/> (Last checked on December 08, 2016)
- [16] <http://weblog.cenriqueortiz.com/touch/2011/02/20/mobility-2011-the-year-of-nfc/> (Last checked on October 7, 2016)
- [17] Haselsteiner, E.; Breitfub, K. Security in near field communication (NFC). In *Proceedings of the Workshop on RFID Security*, Graz, Austria, 12–14 July 2006; pp. 12–14.



- [18] Agrawal, P.; Bhuraria, S. *Near Field Communication. SETLabs Breifings* **2012**, *10*, 67–74.
- [19] Du, H. *NFC technology: Today and tomorrow. Int. J. Future Comput. Commun.* **2013**, *2*, 351–354
- [20] Falke, O.; Rukzio, E.; Dietz, U.; Holleis, P.; Schmidt, A. *Mobile Services for Near Field Communication; Tech. Rep., LMU-MI-2007-1; University of Munich, Department of Computer Science, Media Informatics Group: Munich, Germany, 2007. Available online: <http://www.mmi.ifi.lmu.de/pubdb/publications/pub/falke2007mobileServicesTR/falke2007mobileServicesTR.pdf> (Last checked on November 17, 2016)*
- [21] Moscoso, O.Z.; Lekse, D.; Smith, A.; Holstein, L. *Understanding the current state of the NFC payment ecosystem: A graph based analysis of market players and their relations. Enfoque UTE* **2012**, *3*, 13–32.
- [22] Ortiz, S., Jr. *Is near-field communication close to success? Computer* **2006**, *39*, 18–20.
- [23] *NFC Forum, www.nfc-forum.org. Available online: <http://www.nfc-forum.org/resources/faqs#howwork>*
- [24] Fenn, J. *Hype Cycle for Emerging Technologies, 2010. Gartner Research. Available online: <http://www.chinnovate.com/wp-content/uploads/2011/09/Hype-Cycle-for-Emerging-Technologies-2010.pdf> (Last checked on August 16, 2016)*
- [25] <http://www.mobitel.lk/nfc-solutions> (Last checked on March 08, 2017)
- [26] <http://www.millenniumit.com/what-we-do/systems-integration/our-business-areas/near-field-communications-solutions> (Last checked on March 08, 2017)
- [27] <https://www.dialog.lk/browse/businessInner.jsp?id=onlinefld70071> (Last checked on March 10, 2017)
- [28] Gabriella Arcese, Giuseppe Campagna , Serena Flammini and Olimpia Martucci “Near Field Communication: Technology and Market Trends”, Department of Business Studies, Roma Tre University, September 5, 2014
- [29] Gerald Madlmayr, “Near Field Communication: State of Standardization”, NFC Research Lab, Hagenberg, March 26, 2008
- [30] NFC Forum, “Essentials for Successful NFC Mobile Ecosystems”, October 2008
- [31] David Tushie, “An Introduction to NFC Standards”, October 2012
- [32] [http://www.di-mgt.com.au/rsa\\_alg.html](http://www.di-mgt.com.au/rsa_alg.html) (Last Checked on June 08,2017)