Mohamed Khider University of Biskra
Faculty of Exact Sciences
Department of Computer Science

MASTER THESIS

Speciality : Master - Software Engineering and Distributed Systems - Ref : P1393/2026

TITLE

SmartCard Validator & Withdrawal Terminal

Prepared and defended by

Nour elhouda GAIRAA

Manar HOUHOU

Serine MEZOURI

Defense date : 08/06/2026

DEFENSE COMMITTEE

Full Name	Grade	Role
Djemaa BOUKHLOUF	MCB	**President**
Laid KAHLOUL	Prof	**Supervisor**
Meryem BERGHIDA	MCB	**Examiner**
Faouzia HAGAIN	vacataire	**Incubator Representative**

Academic Year : 2025/2026

Acknowledgements

First and foremost, we would like to express our heartfelt thanks and appreciation to **ALLAH**, the Almighty, for granting us health, power, courage, and patience throughout our journey. We would not have been able to accomplish this without His blessing and guidance.

We would like to express our sincere and deepest appreciation to our supervisor, Professor **Laid Kahloul**, for his precious guidance and support. We would not have been able to accomplish this without his guidance and support.

We would like to express our sincere and deepest appreciation to the members of the jury for their precious time and guidance. Thank you for reviewing our work and enriching it with your precious ideas and comments.

We would like to express our sincere and deepest appreciation to our families, the **Houhou** family, **Mezouri** family, and **Gairaa** family, for their precious love, guidance, and sacrifices. We would not have been able to accomplish this without you.

From me, Manar Houhou : A heartfelt and sincere acknowledgment of thanks and appreciation to my dear father, **Adem Houhou**. Thank you for your precious support, sacrifices and my mother **Benabdi Houda** Thank you for your support and prayers.

From me, Gairaa Nour Elhouda : I would like to express my deepest gratitude to my beloved mother, **Zohra Elhadj Massoud**, and my dear father, **Dr Gairaa Mohammed**, for their love, encouragement, sacrifices, and constant support.

From me, Serine Mezouri : I would like to dedicate this work to my dear mother, **Ghemri Saliha**, my father, **Atef Mezouri**, and my aunt, **Ghemri Isma**, for their love, support, and encouragement throughout my journey.

To everyone who believed in us, supported us, and stood by us—thank you.

Manar Houhou
Serine Mezouri
Nour Elhouda Gairaa

Dedication

To those who held our hands through this, even from a distance.

To our parents—this is just as much yours as ours. Thank you for every sacrifice, every late night worrying, every time you believed in us even when we couldn't believe in ourselves.

To our families—you are our roots. Thank you for loving us even in the midst of chaos, for checking in, and for never forgetting to remind us where we come from.

To our friends—our chosen families. Thank you for the calls we never returned, the texts we never replied to, and for sticking around even when we checked out on you in favor of our work.

This is for you. Always.

Abstract

Every year, thousands of Algerian citizens travel abroad for tourism purposes. To support these trips, the state grants an annual tourism allowance of 750 euros. Today, this amount is delivered manually in different bank branches located at airports, seaports, and land borders. The process often involves long queues, administrative delays, and a high operational burden on staff. Meanwhile, banks have to contend with major logistical challenges in the transportation of large amounts of euros, which are transported by armored trucks under the escort of police-an expensive, risky, and complicated operation.

In the context of national digital transformation, modernizing this procedure has become a priority. This project proposes the development of a Smart Tourism-Card Activation device, an automated system able to identify the traveler, validate eligibility, and load directly the 750€ allocation on a secure smart card. This avoids cash distribution and diminishes altogether the need for physical euro transport.

The proposed solution improves security, simplifies bank operations, enhances traceability, and reduces waiting times for travelers. By integrating embedded systems, secure card-reading technology, and a centralized database, the machine provides a faster, safer, and more transparent alternative to the current manual process. This work demonstrates how digital financial automation can significantly strengthen both service efficiency and national financial logistics.

The proposed solution will improve security, efficiency in the way tourists are served, traceability of transactions, and reduced waiting times at tourist spots and on transport modes.

With the integration of smart card validation equipment, RFID/NFC card reading,GPS location tracking technology, a mobile application, and a management platform, the solution promises a more efficient, secured, and transparent way of conducting business as opposed to the traditional cash-based and manual way of processing tickets.

Keywords

Smart card , Tourism-Card, Activation device ,RFID/NFC , Geolocation (GPS) , Tourists , Embedded systems , Iot , Cloud Coumputing .

Résumé

Chaque année, des milliers d'Algériens voyagent à l'étranger à des fins touristique. Afin de soutenir ces déplacements, l'État leur verse une allocation touristique annuelle de 750 euros. Actuellement, cette somme est distribuée manuellement dans différentes agences bancaires situées dans les aéroports, les ports et aux frontières terrestres. Ce processus engendre souvent de longues files d'attente, des retards administratifs et une charge de travail importante pour le personnel. Parallèlement, les banques doivent faire face à d'importants défis logistiques liés au transport de ces sommes considérables d'euros, acheminées par fourgons blindés sous escorte policière – une opération coûteuse, risquée et complexe.

Dans le cadre de la transformation numérique nationale, la modernisation de cette procédure est devenue une priorité. Ce projet propose le développement d'un dispositif d'activation de la Carte de Tourisme Intelligente, un système automatisé capable d'identifier le voyageur, de vérifier son éligibilité et de charger directement l'allocation de 750 euro sur une carte à puce sécurisée. Ceci permet d'éviter la distribution d'espèces et de réduire considérablement le besoin de transport physique d'euros.

Grâce à l'intégration d'équipements de validation de cartes à puce, de la lecture de cartes RFID/NFC, de la géolocalisation GPS, d'une application mobile et d'une plateforme de gestion, cette solution promet une gestion plus efficace, sécurisée et transparente que le système traditionnel de billetterie, basé sur les espèces et le traitement manuel.

Table des matières

Acknowledgements 1

Abstract 4

List of figures 11

List of tables 12

1 General introduction 13
- 1.1 Context and problematic of this project . . . 13
- 1.2 Objective of this project . . . 13
- 1.3 Target-audience . . . 13
- 1.4 Presentation of start up . . . 14
- 1.5 Related works . . . 14
  - 1.5.1 HDFC forex card . . . 14
  - 1.5.2 Travel card . . . 15
  - 1.5.3 Travelex travel money card . . . 15
- 1.6 Organization of the dissertation . . . 16
  - 1.6.1 Chapter 2 : Technical background . . . 16
  - 1.6.2 Chapter 3 : System design and analysis . . . 16
  - 1.6.3 Chapter 4 : Implementation . . . 16
  - 1.6.4 Chapter 5 : Conclusion and perspectives . . . 16
- 1.7 Conclusion . . . 16

2 Technical background 18
- 2.1 Introduction . . . 18
- 2.2 Internet of thing . . . 18
  - 2.2.1 Definition of IoT . . . 18
  - 2.2.2 The architecture of IoT . . . 18
  - 2.2.3 Three-layer architecture . . . 18
  - 2.2.4 Four-layer architecture . . . 19
  - 2.2.5 Five-layer architecture . . . 20
  - 2.2.6 The elements of IoT . . . 20
- 2.3 Cloud computing . . . 22
  - 2.3.1 What is cloud computing ? . . . 22
  - 2.3.2 Another definitions of cloud computing . . . 23
  - 2.3.3 Architecture of cloud computing . . . 23
  - 2.3.4 Cloud computing benefits for businesses [47] . . . 23
- 2.4 NFC technology . . . 24

2.4.1 Why NFC technology . . . 24
2.4.2 How it works . . . 24
2.5 NFC smart cards . . . 24
2.5.1 The definition of a smart card . . . 25
2.5.2 Contactless smart cards . . . 25
2.6 GPS and geolocation . . . 25
2.6.1 Concept of geolocation . . . 25
2.6.2 Geolocation techniques . . . 26
2.6.3 GPS system . . . 28
2.6.4 Advantages of GPS integration . . . 28
2.7 Conclusion . . . 28

3 System design and analysis **29**
3.1 Introduction . . . 29
3.2 Needs analysis . . . 29
3.2.1 The actors of the system . . . 29
3.2.2 Functional needs . . . 30
3.2.3 Non-functional needs . . . 31
3.3 Data modeling and processing . . . 32
3.3.1 Entity relationship model . . . 32
3.3.2 Relational model . . . 33
3.3.3 Data dictionary . . . 34
3.3.4 UML (Unified Modeling Language) . . . 37
3.4 System design . . . 43
3.4.1 General architecture . . . 43
3.4.2 Architecture of the card validation process . . . 44
3.4.3 Electronic architecture . . . 44
3.4.4 Proposed network architecture for atm connectivity . . . 45
3.5 Conclusion . . . 46

4 Implementation **47**
4.1 Introduction . . . 47
4.2 Programming languages . . . 47
4.2.1 Cascading style sheets (CSS) . . . 48
4.2.2 React native . . . 48
4.2.3 React . . . 48
4.2.4 C++ . . . 49
4.3 Development tools and frameworks . . . 49
4.3.1 PgAdmin database . . . 49
4.3.2 Arduino ide . . . 50
4.3.3 Node.js . . . 50
4.4 The electronic equipment. . . . 51
4.4.1 ESP32 microcontroller . . . 51
4.4.2 Keypad (matrix 3*4) . . . 51
4.4.3 NFC/RFID reader . . . 52
4.4.4 Active buzzer . . . 52
4.4.5 Display 16*2 HD 44780 . . . 53
4.4.6 3.7V battery . . . 53
4.4.7 GT-U7 GPS module . . . 53

4.5 The main algorithms of the system . . . 54
4.5.1 Pseudo algorithms on the application side . . . 54
4.5.2 Pseudo algorithms on the device side . . . 59
4.6 Mobile application . . . 63
4.6.1 Login page . . . 63
4.6.2 Dashboard page . . . 64
4.6.3 Transactions page . . . 68
4.6.4 Location page . . . 69
4.6.5 Statistics page . . . 70
4.6.6 Profile page . . . 71
4.7 Web application . . . 73
4.7.1 Home page . . . 74
4.7.2 Sign in / Sign up page . . . 74
4.7.3 Tourism dashbaord page . . . 75
4.7.4 Transaction management page . . . 77
4.7.5 Profile and account settings page . . . 79
4.7.6 Analytics page . . . 80
4.7.7 Administrator dashboard . . . 80
4.7.8 User management page . . . 81
4.7.9 Card's request management page . . . 81
4.7.10 Cards management page . . . 82
4.7.11 Analytics page . . . 82
4.7.12 ATM network page . . . 82
4.7.13 Sub administrator dashboard . . . 83
4.8 Integration of GPS in the smartcard validator ATM . . . 83
4.9 Security protocols . . . 84
4.9.1 Authentication and authorization . . . 84
4.9.2 Data protection . . . 85
4.9.3 Transport layer security . . . 85
4.9.4 External communication . . . 86
4.9.5 Database communication . . . 86
4.9.6 Email communication . . . 87
4.9.7 File upload security . . . 87
4.9.8 AI based fraud detection . . . 88
4.10 Product prototype . . . 89
4.11 System maintenance strategy . . . 90
4.11.1 Objectives of maintenance . . . 90
4.11.2 Maintenance categories . . . 90
4.11.3 Hardware maintenance . . . 92
4.11.4 Software maintenance . . . 93
4.11.5 Self diagnostic system . . . 93
4.11.6 Remote monitoring system . . . 94
4.11.7 Database backup and recovery . . . 94
4.12 Conclusion . . . 94

5 Conclusion and Perspectives **96**
5.1 Conclusion . . . 96
5.2 Perspectives . . . 96

Table des figures

1.1 Multicurrency forex card [4] . . . 14
1.2 Travel card [5] . . . 15
1.3 Travel money card [52] . . . 15

2.1 Three-layer architecture of IoT [23] . . . 19
2.2 Four-layer architecture of IoT [23] . . . 20
2.3 Architectures of IoT [23] . . . 21
2.4 The elements of IoT [35] . . . 22
2.5 The model of cloud computing [47] . . . 22
2.6 The architecture of cloud computing [44] . . . 23
2.7 Illustration of how NFC works, showing the reader's electromagnetic field powering the passive NFC tag and enabling data exchange [24]. . . . 25
2.8 A contactless smart card showing the embedded microchip and antenna [16]. 25
2.9 The principle of operation of the Global Positioning System (GPS) is based on measuring the distance from the receiver to several satellites [12]. . . . 26
2.10 Principle of GSM-based geolocation using cellular network signals to estimate the position of a mobile device [13]. . . . 27
2.11 Geolocation by IP Address [14]. . . . 27

3.1 Relational Model Diagram . . . 34
3.2 Use case diagram of application . . . 38
3.3 Use case diagram of device . . . 38
3.4 Sequence diagram of application (1) . . . 39
3.5 Sequence diagram of application (2) . . . 39
3.6 Sequence diagram of application (3) . . . 40
3.7 Sequence diagram of device (1) . . . 40
3.8 Sequence diagram of device (2) . . . 41
3.9 Sequence diagram of device (3) . . . 41
3.10 Class diagram of device . . . 42
3.11 Class diagram of application . . . 42
3.12 Deployment diagram of device . . . 43
3.13 General architecture of the system . . . 43
3.14 Architecture of the card validation process . . . 44
3.15 Architecture of the system . . . 44
3.16 Proposed telecom network architecture for ATM connectivity. . . . 46

4.1 Logo of the CSS language [46] . . . 48
4.2 Logo of the React Native [49] . . . 48
4.3 Logo of the react framework [19] . . . 49
4.4 Logo of the C++ programming language [15] . . . 49

4.5 Logo of pgAdmin [20] . . . 50
4.6 Logo of Arduino IDE [21] . . . 50
4.7 Logo of Node.js [17] . . . 51
4.8 Model ESP32 [22] . . . 51
4.9 Keypad(3*4) [39] . . . 52
4.10 NFC/RFID reader [37] . . . 52
4.11 Active buzzer [30] . . . 53
4.12 Display 16*2 HD 44780 [39] . . . 53
4.13 3.7V battery . . . 53
4.14 GT-U7 GPS module [18] . . . 54
4.15 Authentication and guide pages . . . 64
4.16 Dashbaord page (01) . . . 65
4.17 Dashbaord page (02) . . . 65
4.18 Renew card section (Dashboard Page) . . . 66
4.19 Block card section (Dashboard page) . . . 66
4.20 Change PIN of card step (1) . . . 66
4.21 Change PIN of card step (2) . . . 66
4.22 Card management features in dashboard . . . 66
4.23 Forget PIN of card (1) . . . 67
4.24 Forget PIN of card (2) . . . 67
4.25 Alert types . . . 67
4.26 WhatsApp notification . . . 68
4.27 Email notification (1) . . . 68
4.28 Email notification (2) . . . 68
4.29 Email notification (3) . . . 68
4.30 Notification system . . . 68
4.31 Transaction page . . . 69
4.32 Transactions file downloaded . . . 69
4.33 Location Page . . . 70
4.34 Statistics page views . . . 71
4.35 Profile page (1) . . . 72
4.36 Profile page (2) . . . 72
4.37 Help center section . . . 72
4.38 Security section . . . 72
4.39 Profile and settings sections . . . 72
4.40 Notifications setting section . . . 73
4.41 General setting section . . . 73
4.42 Settings sections . . . 73
4.43 QR code of application . . . 73
4.44 IA chatbot assistance . . . 73
4.45 Settings Sections . . . 73
4.46 Home page (1) . . . 74
4.47 Home page (2) . . . 74
4.48 Home page (3) . . . 74
4.49 Account creation . . . 75
4.50 Login page . . . 75
4.51 Renew card section (dashbaord page) . . . 76
4.52 Block card section (dashbaord page) . . . 76

4.53 View details section (dashbaord page) . . . 76
4.54 Change pin of card section (dashbaord page) . . . 76
4.55 Notifications section (dashbaord page) . . . 76
4.56 Request for new tourism card . . . 77
4.57 Search transactions page . . . 77
4.58 Download PDF/CSV section . . . 78
4.59 Filter options section . . . 78
4.60 Transactions details section . . . 78
4.61 Report issue of transactions . . . 79
4.62 Transaction management page . . . 79
4.63 Pdf file of transactions downloaded . . . 79
4.64 Profile and account settings page(1) . . . 80
4.65 Profile and account settings page(2) . . . 80
4.66 Analytics page(1) . . . 80
4.67 Analytics page(2) . . . 80
4.68 Admin dashboard page(1) . . . 81
4.69 Admin dashboard page(2) . . . 81
4.70 User management page(1) . . . 81
4.71 User management page(2) . . . 81
4.72 Card's request management page(1) . . . 82
4.73 Card's request management page(2) . . . 82
4.74 Cards management page(1) . . . 82
4.75 Cards management page(2) . . . 82
4.76 Analytics page (1) . . . 82
4.77 Analytics page (2) . . . 82
4.78 ATM network page . . . 83
4.79 Sub administrator dashboard(1) . . . 83
4.80 Sub administrator dashboard(2) . . . 83
4.81 Picture of our activation ATM . . . 89
4.82 Picture of our tourism card . . . 89
4.83 Picture of our purshace device . . . 90

Liste des tableaux

3.1 Data dictionary(1) 35
3.2 Data dictionary(2) 36
3.3 Data dictionary(3) 37

Chapitre 1

General introduction

1.1 Context and problematic of this project

With the increasing demand for the tourism allowance provided by the government in foreign currency especially in euros, banks are facing tremendous pressure in all operational branches : airport, seaport, and land offices. Banks have to continually address problematic situations due to rigid regulatory constraints, low availability in the country, and increasing customer needs. All this gets even more complicated because in three days, the value of the euro can change significantly, which puts banks in a hard place to estimate what their customers will need and how to manage the reserves efficiently. Besides, internal transportation of cash between branches often requires armored vehicles and police escorts, showing how sensitive and at what cost this mission can be. Such practices lead to delays, very high costs, and organizational tension on banking staff, who have to explain the limited resources against high demand. Under these circumstances, technological tools able to enhance the monitoring, forecasting, and distribution of currency reserves became vital to enhancing the operation performance of banks and ensuring higher quality of service within all units.

1.2 Objective of this project

This project aims to develop an automated card-activation system that offers a secure, efficient, and reliable alternative to the current manual process at airports, seaports, and land borders. More specifically, this system will avoid fraud, theft, and human error in the manual handling of cash, Operating 24/7 without dependence on the bank staff's presence. It cuts waiting times for customers by automating identity verification and card activation, and it enables the bank to monitor all transactions in real time to ensure full traceability and accountability. The aim is to improve user convenience and operational efficiency while enhancing security in relation to financial services at international travel points.

1.3 Target-audience

Banking institutions are the primary users of the proposed system since they handle transaction processing, card issuance, account management, and foreign currency exchange operations effectively. This system aids them in alleviating operational burdens,

enhancing service quality, and providing improved oversight and tracking of financial transactions.

Meanwhile, travelers gain from this system by having a secure and convenient means to manage their finances while abroad, minimizing delays and easing access to foreign currency.

Additionally, the system is designed to function at border control locations (airports, seaports, and land crossings), where officials can securely activate and validate the TourismCard with the Smart Card Validator device.

1.4 Presentation of start up

The proposed start-up business, **Tourism Card validator solution**, is an innovative technology-based business specializing in the development of secure digital systems for the Banking institutions .

The start-up business seeks to revolutionize the way people spend while touring through the development of an integrated system consisting of the following components :

- **Tourism smart card** of 750 Euro equivalent for the tourism sector.
- **Smart card validator device** based on NFC a technologies.
- **Mobile application** for the tourism sector.
- **Web platform** for administrators/regulatory authorities and tourism also .

1.5 Related works

1.5.1 HDFC forex card



FIGURE 1.1 – Multicurrency forex card [4]

In August, 2014 the HDFC Bank introduced "ForexPlus' card for people making the Haj and Umrah pilgrimages. The card was launched with the objective of letting the pilgrims making all payments during their pilgrimage and withdraw money from ATMS as well. "With the launch of the prepaid forex card, we are offering pilgrims to Haj and Umrah a customised product to suit their ever-evolving requirements. They can make payments in a safe and easy manner, and also avail of the exclusive deals offered on the card [2].

1.5.2 Travel card



FIGURE 1.2 – Travel card [5]

— A Prepaid Visa Card issued by Standard Chartered Bank against Travel Quota entitlement
— A Convenient Alternative to Cash Foreign currencies and Traveller's Cheques.
— Attractive Card Design
— Minimum value is US$ 100 and Maximum is US$ 1,000 for SAARC (& Myanmar) countries and US$ 3,000 for Non-SAARC countries
— Can be used to withdraw money at over 850,000 Visa ATMs worldwide.
— Can be used at over 13 million outlets across the globe that accepts VISA card ONLINE.
— Anyone above 18 can purchase Travel Card.
— No need to maintain account/card with SCB.
— Safer than Cash and TC as it can be replaced if lost/stolen.
— Can be used multiple times until spending value is exhausted.
— No Air-ticket / Visa required for getting a Travel card.
— Simple Documentation (no TM Form) [34].

1.5.3 Travelex travel money card



FIGURE 1.3 – Travel money card [52]

Travelex offers prepaid travel cards. These cards allow users to load multiple currencies 11 onto a single card, providing convenience and security during international travel. The cards can be used for purchases and cash withdrawals, often offering competitive exchange rates and reduced fees compared to traditional debit or credit cards. Travelex also provides money transfer services, allowing customers to send money abroad or receive funds from overseas. These services can be accessed online or through Travelex

locations, offering flexibility and convenience for individuals who need to transfer money internationally. Travelex is known for its extensive network of physical locations, with many branches located in airports, shopping centers, and popular tourist destinations. This accessibility makes it convenient for travelers to access their services, particularly for last-minute currency needs. In conclusion, Travelex is a prominent foreign exchange provider with a global presence, offering currency exchange, prepaid travel cards, and money transfer services. Its extensive network of locations, competitive rates, and convenient options make it a popular choice for travelers and individuals in need of foreign currency services [42].

1.6 Organization of the dissertation

The organization of the dissertation is as follows.

1.6.1 Chapter 2 : Technical background

In the second chapter, we introduce the technical background of the project. This includes key concepts on IoT, embedded systems, smart cards, secure financial transactions, and database management, with an emphasis on connected verification devices.

1.6.2 Chapter 3 : System design and analysis

In the third chapter, we describe the system design and analysis. This chapter presents the overall architecture, workflows, and diagrams illustrating interactions between clients, administrators, banks, and the smart card verification device.

1.6.3 Chapter 4 : Implementation

In the fourth chapter, we explain the implementation of the project. It details the development tools, programming languages, and algorithms used, and includes screenshots and images of the web platform, mobile application, and the verification device in operation.

1.6.4 Chapter 5 : Conclusion and perspectives

In the fifth chapter, we provide the conclusion of the dissertation, highlighting the main achievements of the project and offering perspectives for future enhancements.

1.7 Conclusion

The problems associated with the distribution of the annual 750€ tourism allowance have been discussed in this chapter. The existing method results in long queues, delay in the distribution process, logistical difficulties related to transporting euros, and security threats. In this context, we have suggested the implementation of a SmartCard Validator System that would automate the entire distribution process. With the new method, the cash handover process will be replaced by the automatic loading of money into the traveler's smart card. As a result, logistics, security threats, and fraudulent activities can be

minimized. Moreover, with the help of the proposed solution, travelers would be able to get access to their money at any time and from any place. The proposed solution would also allow banks to control transactions online, ensuring transparency and security.

Chapitre 2

Technical background

2.1 Introduction

The increasing number of Algerian citizens traveling abroad for tourism and other purposes has created a growing need for secure and efficient financial services at border points such as airports, seaports, and land crossings. Traditional manual procedures for handling the tourism allowance often suffer from delays, lack of transparency, and security limitations.

To address these issues, this project proposes the **SmartCard validator system**, a connected solution based on a Smart Tourism Card and an intelligent validator device. The system integrates several modern technologies such as NFC smart cards, Internet of Things (IoT), cloud computing, and GPS to ensure secure activation, real-time monitoring, and reliable communication between devices and the central platform.

This chapter presents the main technical background used in the project, including IoT, cloud computing, NFC smart cards, and GPS technology, which form the technological foundation of the proposed system.

2.2 Internet of thing

2.2.1 Definition of IoT

IoT is one of the enabling technologies of the "Industry 4.0". Its goal is the connection of humans with machines and smart technologies. The Internet of Things (IoT) refers to the vast interconnected network of computer devices (e.g., sensors) which exchange large amounts of data at rapid speed [27].

2.2.2 The architecture of IoT

IoT systems are structured in various ways. The simplest uses a three-layer design comprising perception, network, and application layers. Today, however, a five-layer architecture has become more common. We will explore both models in detail.

2.2.3 Three-layer architecture

As indicated by its name, this model primarily consists of three layers. Following the definitions provided by the authors of [35], we will describe each layer individually before

presenting them in Figure below.

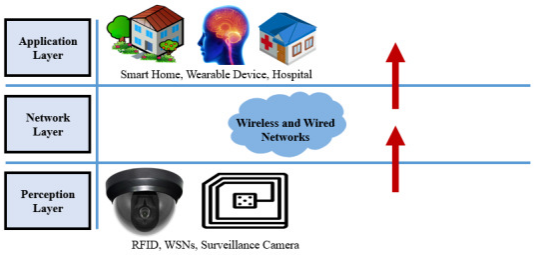


FIGURE 2.1 – Three-layer architecture of IoT [23]

1. Perception layer : It is also known as a sensor layer. It works like people's eyes, ears and nose. It has the responsibility to identify things and collect the information from them. There are many types of sensors attached to objects to collect information such as RFID, 2-D barcode and sensors. The sensors are chosen according to the requirement of applications. The information that is collected by these sensors can be about location, changes in the air, environment, motion, vibration, etc. However, they are the main target of attackers who wish to utilize them to replace the sensor with their own.
2. Network layer : Network layer is also known as transmission layer. It acts like a bridge between perception layer and application layer. It carries and transmits the information collected from the physical objects through sensors. The medium for the transmission can be wireless or wire based. It also takes the responsibility for connecting the smart things, network devices and networks to each other. Therefore, it is highly sensitive to attacks from the side of attackers.
3. Application layer :

   Application layer defines all applications that use the IoT technology or in which IoT has deployed. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, etc. It has the responsibility to provide the services to the applications. The services may be varying for each application because services depend on the information that is collected by sensors.

2.2.4 Four-layer architecture

The reason to make a fourth layer is the security in architecture of IoT. Information is sent directly to the network layer in three-layer architecture. Due to sending information directly to the network layer, the chances of getting threats increase. Due to flaws that were available in three-layer architecture, a new layer is proposed. In four-layer architecture, information is sent to a support layer that is obtained from a perception layer. The support layer has two responsibilities. It confirms that information is sent by the authentic users and protected from threats. There are many ways to verify the users and the information. The most commonly used method is the authentication. It is implemented by using pre-shared secrets, keys and passwords. The second responsibility of the support layer is sending information to the network layer. The medium to transmit information from the support layer to network layer can be wireless and wire based [27]. Figure below describe Four-layer architecture of IoT.

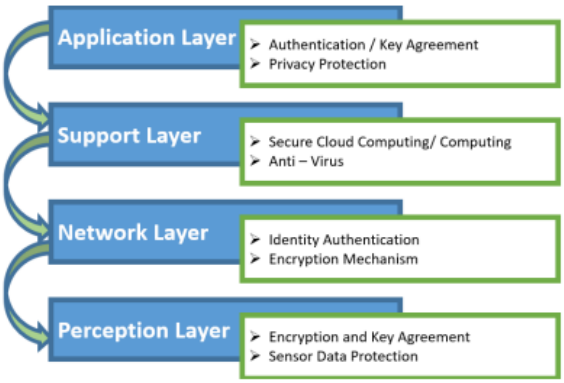


FIGURE 2.2 – Four-layer architecture of IoT [23]

2.2.5 Five-layer architecture

The four-layer architecture played an important role in the development of IoT. There were also some issues regarding security and storage in four-layer architecture. Researchers proposed five-layer architecture to make the IoT secure [49–51]. It has three layers like previous architectures whose names are perception layer, transport layer and application layer. It also has two more layers. The names of these newly proposed layers are processing layer and business layer. It is considered that the newly proposed architecture has the ability to fulfill requirements of IoT. It also has the ability to make the applications of IoT secure [35].

1. Processing Layer :

   The processing layer is also known as a middleware layer. It collects the information that is sent from a transport layer. It performs processing onto the collected information. It has the responsibility to eliminate extra information that has no meaning and extracts the useful information. However, it also removes the problem of big data in IoT. In big data, a large amount of information is received which can affect performance of IoT.

2. Business Layer :

   The business layer refers to an intended behavior of an application and acts like a manager of a whole system. It has responsibilities to manage and control applications, business and profits models of IoT. The user's privacy is also managed by this layer. It also has the ability to determine how information can be created, stored and changed. Vulnerability in this layer permits the attackers to misuse an application by avoiding the business logic.

2.2.6 The elements of IoT

Understanding the core components of IoT provides clarity on its true purpose and operation. This section outlines six essential elements—identified in [35] that enable IoT functionality : definition, detection, communication, computing, services, and semantics.

1. Identification :

   Identification offer explicit identity for each object within network. There are two processes in identification ; naming and addressing. Naming refers as name

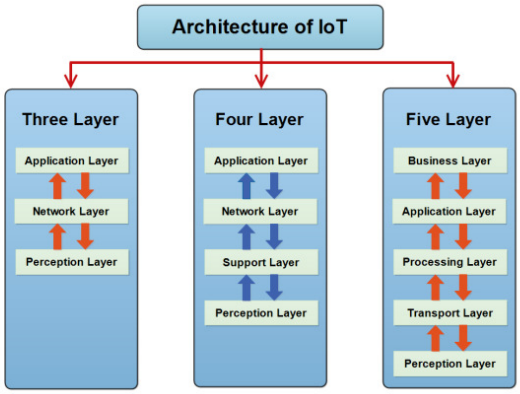


FIGURE 2.3 – Architectures of IoT [23]

of the object while addressing is the unique address of specific object. These both terms are very different from each other because two or more objects may have same name but always different and unique address. There are many methods available that provide the naming facility to the objects in the network such as electron products codes (EPC) and ubiquitous codes . To assign the unique address to each object, IPv6 is used. Firstly, IPv4 was used to assign the address but it could not fulfill the need of addressing due to large amount of IoT devices. Therefore, IPv6 is used because it uses 128 bit number addressing scheme.

2. Sensing : The process of collecting information from objects is known as sensing. The collected information is sent to the storage media. There are many sensing devices to collect the information from objects such as actuators, RFID tags, smart sensors, wearable sensing devices, etc.

3. Computation :

   Computation is performed on the collected information from the objects by using sensors. It is used to remove unnecessary information that is not needed. Many hardware and software platforms are developed to perform the processing in applications of IoT. For hardware platforms, Audrino, Rasperry Pi and Intel Galileo are used, while, for software platforms, the operating system plays an important role to perform the processing. There are many types of operating systems that are used like Tiny OS , Lite OS , Android, etc.

4. Communication :

   Communication is one of the main purposes of IoT in which different devices are connected to each other and communicate. In communication, devices may send and receive messages, files and other information. There are many technologies that provide facility of communication like Radio Frequency Identification (RFID) , Near Field Communication (NFC) , Bluetooth , Wi-Fi and Long Term Evolution (LTE) .

5. Services :

   There are four types of services that are provided by the IoT applications [30,31]. The first one is an identity-related service. It is used to get the identity of objects that have sent the request. Information aggregation is another service whose purpose is to collect all the information from objects. Processing is also performed by the aggregation service. The third service is a collaborative service

that makes decisions according to the collected information and sends appropriate responses to the devices. The last service is ubiquitous service, which is used to respond the devices immediately without rigidity about time and place.

6. Semantics : : It is the responsibility of IoT to facilitate users by performing their tasks. It is the most important element of IoT to fulfill its responsibilities. It acts like the brain of IoT. It gets all information and makes appropriate decisions to send responses to the devices.

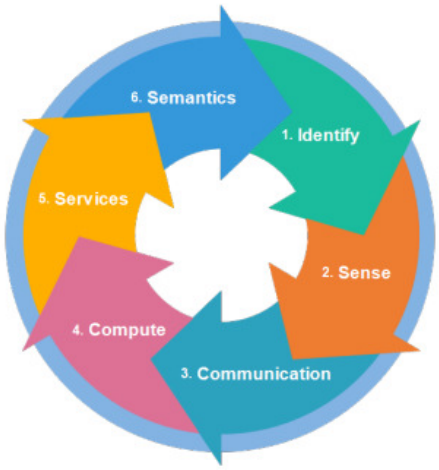


FIGURE 2.4 – The elements of IoT [35]

2.3 Cloud computing

2.3.1 What is cloud computing ?

Cloud computing is a term used to describe both a platform and type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Servers in the cloud can be physical machines or virtual machines. Advanced clouds typically include other computing resources such as storage area networks (SANs), network equipment, firewall and other security devices.

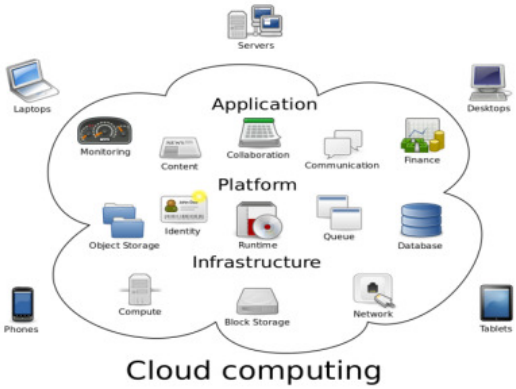


FIGURE 2.5 – The model of cloud computing [47]

2.3.2 Another definitions of cloud computing

A cloud is a pool of virtualized computer resources. A cloud can [8] :

1. Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications.
2. Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines.
3. Monitor resource use in real time to enable rebalancing of allocations when needed.
4. Support redundant, self-recovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures.

2.3.3 Architecture of cloud computing

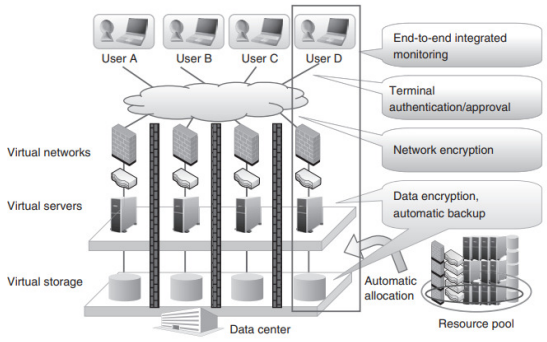


FIGURE 2.6 – The architecture of cloud computing [44]

2.3.4 Cloud computing benefits for businesses [47]

1. Enhanced Security : The security of information put away in the cloud is a significant concern. Cloud computing give high security by utilizing the information encryption, solid access controls, key administration, and security insight .It also provide the Artificial intelligence based security by judging the nature of the user.
2. . Backup and Recovery :A cloud-based platform with built-in redundancy can save the business from loss of the data .Lost of data leads to loss of productivity, revenue, and brand reputation . Cloud keeps the data secure, backed-up and easily accessible. It helps to overcome the loss of disasters and resume the business in a streamlined way . Cloud-based services provide instant data recovery for all types of emergency .
3. Availability of Resources :The services on cloud are commonly accessible all day, every day and open from various programs and gadgets (i.e., work area, PC, Smartphone, iPad) in some random time zone. This gives colossal adaptability for everybody to lead their work.
4. Mobility : Cloud computing allows its customers to get products and services from anyplace and whenever through cell phones. On the off chance that the clients travel, he is able to access the services through their smart phones and laptops [9]. And if business switches to another location the same services are available without any efforts of transport.

5. Scalability : Cloud Computing provides services as per demand of clients or businesses.It permits upscaling or downscaling the administrations as indicated by the interest, traffic, and regular spikes. Cloud gives the adaptable engineering your business needs [15]. The way that your business will increment in the coming time, it is essential to scale the business as it develops. This handle expanded outstanding tasks at hand and satisfy the fluctuating needs in the pinnacle season . These varieties of cloud computing services give us adaptability.

2.4 NFC technology

Near Field Communication (NFC) is a technology that allows two devices to exchange information wirelessly at close range. More precisely, NFC is a set of technical specifications and standards for transferring information between two proximate objects via the inductive coupling of radio frequency fields at 13.56 MHz. NFC evolved out of existing radio-frequency identification (RFID) standards [38].

2.4.1 Why NFC technology

— High Security : The use of NFC is over a very short range, thereby minimizing the chances of unauthorized use.
— Contactless Operation : There is no need for users to physically touch the device.
— Ease of Use : NFC does not require users to physically configure, pair, or use passwords, thereby improving the ease of use.
— Wide Compatibility : The majority of existing smartphone devices support NFC.

2.4.2 How it works

NFC data exchange requires two participating objects : an initiator (or reader) and a target (or transponder). Both the initiator and target must be tuned to the same radio frequency to communicate, so NFC specifications require that all NFC data exchanges occur at 13.56 MHz, the high-frequency (HF) standard commonly used in RFID systems. To launch an NFC exchange, the initiator uses an antenna to emit a radio wave at 13.56 MHz. These radio waves are electromagnetic fields, consisting of both electric and magnetic components, and their properties change as they propagate outward from the antenna. The magnetic field strength decreases rapidly within one wavelength or less from the antenna—this is known as the "near field" in "near field communication," which establishes the proximity requirement for NFC : communication can only occur within this short read range (or operating volume) [38].

2.5 NFC smart cards

Smart cards play a central role in modern electronic payment and identification systems. In the TourismCard project, NFC smart cards are used as the primary medium for secure user identification and financial transactions.

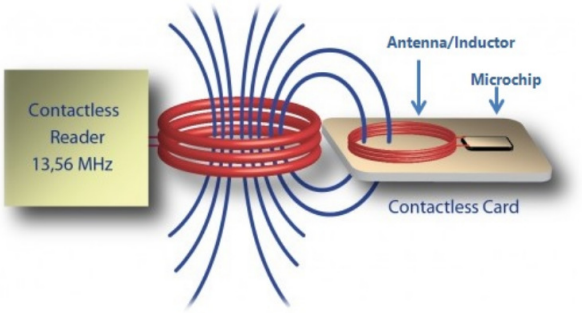


FIGURE 2.7 – Illustration of how NFC works, showing the reader's electromagnetic field powering the passive NFC tag and enabling data exchange [24].

2.5.1 The definition of a smart card

A Smart card is a portable hardware device having the same dimensions of a credit card, 85.60 × 53.98 × 0.76 mm (3.370 × 2.125 × 0.030 in), which can store and process information by an integrated circuit encapsulated on a plastic strip [11].

2.5.2 Contactless smart cards

A contactless smart card is a type of smart card that is processed without a need for physical contact with an external device. It is a combination of a microchip embedded within it and an antenna, which allows the card to be tracked Several wires form this antenna. In contactless smart cards, information is stored in the microchip, which has a secure microcontroller and internal memory. Unlike the contact smart card, the power supply to the contactless smart card is achieved with its embedded antenna. Data exchange between the smart card and an external device such as a smart card reader is performed with the help of this antenna. Electromagnetic fields for the card provide the power ; hence, data exchange occurs between the card and the external device [16].

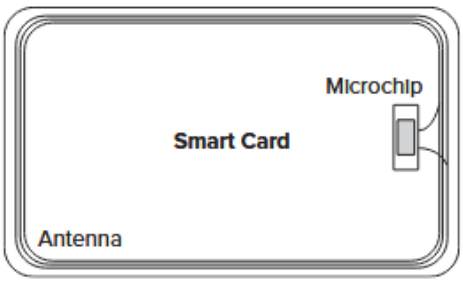


FIGURE 2.8 – A contactless smart card showing the embedded microchip and antenna [16].

2.6 GPS and geolocation

2.6.1 Concept of geolocation

Geolocation consists of locating a resource or an individual on a map or a plan using their geographical coordinates (longitude, latitude, altitude). This operation is executed as reported by authors is carried out using a device capable of being located, such as a GPS

receiver or a satellite positioning system. The recorded positions can be stored within the device and ex- tracted later, or transmitted in real-time to a geolocation software platform. Real-time transmis- sion requires a device equipped with a telecommunication means such as GSM, GPRS, UMTS, radio or satellite, allowing it to send positions at regular intervals. This allows the position of the device to be displayed on a map through a geolocation platform, most often accessible from the internet [1].

2.6.2 Geolocation techniques

2.6.2.1 Satellite geolocation

Satellite interference geolocation plays a critical role in addressing radio interference problems related to satellite communications systems. Traditional interference geolocation approaches are mainly based on time-difference-of-arrival (TDOA) and frequency-difference-of-arrival (FDOA) measurements. However, since new technologies have appeared, such as the widespread use of high-frequency bands, spot beams, emerging large-scale low- Earth orbit satellite constellations, and onboard processing, traditional methods may be unsuitable for modern satellite communications [29].

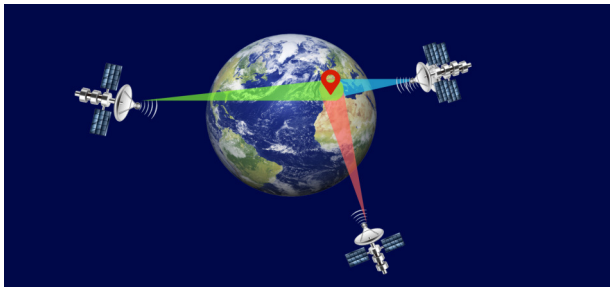


FIGURE 2.9 – The principle of operation of the Global Positioning System (GPS) is based on measuring the distance from the receiver to several satellites [12].

2.6.2.2 Geolocation by GSM

The GSM can be used to be obtained location information without additional external hardware when there is cellular coverage . Location Based Services (LBS) with the popularity is smartphones that have grown rapidly over the past years and market forecasts show similar growth in the near future. As the need for tracking mobiles in our daily life is increasing, it became tracking thousands of users periodically on the scale of minutes, focuses on cheap and cellular networks independent tracking solution that does not need any hardware change within the core network and that can find any mobile terminal [9].

2.6.2.3 Geolocation by wiFi

WiFi geolocation works by comparing the WiFi access points a device is detecting with the locations of mapped WiFi networks stored in a database. Thankfully, WiFi databases tend to be more accu- rate than their IP address counterparts. One study utilizing an iPhone as a test device found that most WiFi geolocation results were between 58 and 74 meters of the actual location. In compari- son, IP databases can have location errors up to 100s of kilometers. Despite its greater accuracy, it is still possible to spoof WiFi

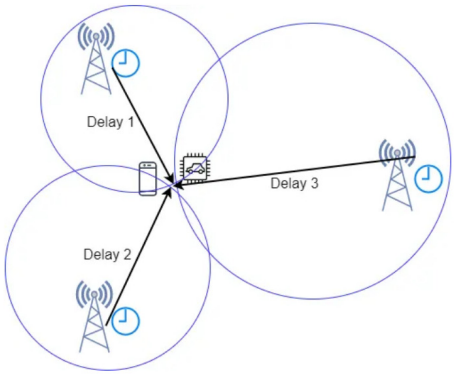


FIGURE 2.10 – Principle of GSM-based geolocation using cellular network signals to estimate the position of a mobile device [13].

geolocation results. For example one method of spoofing WiFi geolocation involves jamming the signals from real WiFi access points while at the same time impersonating access points from another location. However, this form of spoofing requires financial resources, time, and technical know-how far beyond that of the average computer user, and as such remains largely a theoretical risk [48].

2.6.2.4 Geolocation by IP address

IP geolocation is the process of finding geographic loca- tions of Internet Protocol addresses. IP geolocation is widely used today. For example, companies use IP geolocation to limit the content to certain countries (for example, televi- sion and movies that are often licensed differently by the viewer's country) and to customize advertising based on location. Internet researchers use IP geolocation to relate net- work phenomena to countries, such as studying the cultural impacts on social networking, or rates of computer crime by country and policy. Moreover, IP geolocation is essential in law enforcement to identify the appropriate jurisdiction to handle enforcement of computer crime statues. [31].

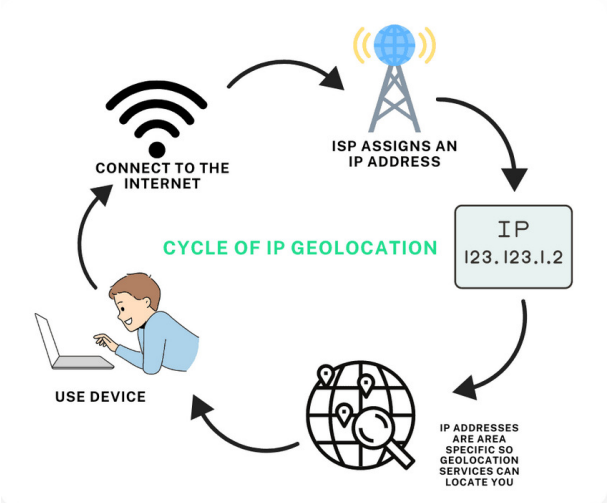


FIGURE 2.11 – Geolocation by IP Address [14].

2.6.3 GPS system

The Global Positioning System (GPS) is a navigation system based on satellite technology. Its fundamental technique involves measuring the ranges between the receiver and a few simultaneously observed satellites, and the positions of the satellites are forecasted and broadcasted along with the GPS signal to the user. Through several known positions (of the satellites) and the measured distances between the receiver and the satellites, the position of the receiver can be deter- mined. The position change, which can also be determined, is then the velocity of the receiver. The most important applications of GPS are positioning and navigation [53].

2.6.4 Advantages of GPS integration

The integration of GPS into the SmartCard Validator ATM provides several advantages :

- Verification of activation location.
- Prevention of unauthorized activation outside border zones.
- Improved traceability and auditing.
- Real-time monitoring of ATM deployment.

2.7 Conclusion

This chapter introduced the main technical concepts used in the SmartCard Validator System. It showed how IoT enables communication between connected devices, how cloud computing supports data storage and processing, and how NFC smart cards provide secure and fast user identification.

It also explained the role of GPS technology in improving tracking and location verification at border points. The combination of these technologies provides a solid technical base for building a secure, efficient, and modern system for managing the tourism allowance in Algeria.

Chapitre 3

System design and analysis

3.1 Introduction

This chapter focuses on the design and analysis of our SmartCard Validator system. The main objective of the system is to provide secure access control by validating smart cards in real time. At the same time, it gives immediate feedback to the user and logs all access events for monitoring and auditing purposes.

Here, we present the system specifications, outline its functional requirements, and describe the design using general architecture diagrams and UML models. This structured approach helps to understand how the system operates and interacts with users and administrators. modeling our system.

3.2 Needs analysis

3.2.1 The actors of the system

Our system involves various actors who interact with the application, the platform, and the Atm device .

Who is the user of our system ?

Answer : The tourist is a dominant actor in the system. Se/he will make use of the smart card and the mobile application in order to request touristic services, check balance, review own traveling history and update personal information.

Who is the system administrator ?

Answer : Administrator : Manage the platform,users, set parameters of the system and transactions, monitor transaction activities, ensure security and availability of system.

Who is the support and maintenance team ?

Answer : This is the team that maintains, provides technical support , can fix hardware,install new software and resolve issues.

Who is the payment service provider ?

Answer : This actor is responsible for transaction of online payments, card recharging operations and transactions in a touristic system.

3.2.2 Functional needs

This section describes the functional requirements of the complete smart card validation system, including the mobile application, the validation device, the central platform, and connected services. The functions are presented according to each actor.

3.2.2.1 Tourist (User)

The tourist interacts with the system through the smart card and the mobile application and can perform the following functions :

- Create and manage a personal account.
- Login and consult card balance.
- Validate the card at authorized terminals.
- View all expired smart cards.
- Change pin of card or emergency block.
- Renew the expired card.
- Request for new tourism card.
- Block the tourism card.
- View usage history and transactions report.
- Receive notifications and alerts.
- Update personal information.
- Analysis report about spending and transactions categories.

3.2.2.2 System administrator

The system administrator is responsible for the entire system, which includes the application, device, and platform. His/her responsibilities include :

- Management of user accounts and smart cards.
- Handling requests related to cards, such as rejecting and approving card's request.
- Configuring system rules and parameters.
- Management of validation terminals and entities.
- Monitoring the system and its transactions.
- Generating reports and performing statistical analysis.
- Management of access rights and permissions.
- Detecting and preventing fraudulent activities.
- Ensuring the security of the system and maintaining backups.

3.2.2.3 Support and maintenance team

The role of the maintenance team is to ensure the reliability and continuity of the system, which includes :

- Maintenance and repair of validation devices.
- Installation of system updates or patches.
- Providing technical support to users .

— Diagnosis and remediation of system failures.
— Ensuring connectivity to the network.

3.2.2.4 Payment service provider

The payment service provider is responsible for all the financial transactions, which include :

— Processing all the online or physical recharge transactions.
— Validating payment transactions.
— Ensuring secure money transfer services.
— Managing refunds or any possible disputes.
— Preventing any possible financial frauds.

3.2.3 Non-functional needs

3.2.3.1 Aesthetic constraints

— The user interface of the mobile application and the platform should have a tourism-oriented thematic design.
— The colors should be appealing and comfortable for the eyes ; dark colors should be avoided.
— The images should be related to tourism, traveling, and associated services.
— The user interface of the device for validation should have a clean, simple, and intuitive design.

3.2.3.2 Ergonomic constraints

— The application should have a user-friendly interface, easily comprehensible and usable by tourists and staff.
— The application interface should be simple, intuitive, and consistent for all users.
— Texts, messages, and information should be clear and easily understandable.
— The application should be compatible with various devices, such as smartphones, tablets, and terminals.

3.2.3.3 Performance

— **Response time :** The system shall respond rapidly with no delays perceived by the user.
— **Transaction processing speed :** Large numbers of validation and transaction operations shall be processed in near-real time.
— The validation terminal shall operate efficiently in offline mode with subsequent data synchronization.

3.2.3.4 Scalability

— The system shall handle an increasing number of users.

3.3 Data modeling and processing

3.3.1 Entity relationship model

The Entity-Relationship (E-R) model is often used as a tool for communication between a designer and an end-user of a database because of its ease of use and its convenience in representation. the popularity of the E-R model for high level design is due to its economy of concepts and belief in entities and relationships as natural modelling concepts [50].

ENTITÉ : User

id : Identifiant unique
FirstName
LastName
email
password
phoneNumber
dateBirth
address
createdAt
isActive
lastLogin

ENTITÉ : Admin

adminID
Name
emailAD
passwordAD

ENTITÉ : Card

cardID
creditLimit
avCredit
expiryDate
state
pin

ENTITÉ : Card_Request

idRequest
requestState
requestDate
adminNotes

ENTITÉ : DOCUMENT

docType
fileName
filePath
fileSize
fileState

ENTITÉ : DEVICE

deviceID
location
batteryLVL

ENTITÉ : TRANSACTION

transID
type
amount
dateTRAN
stateTran
locationTRAN

Associations et cardinalités

— USER (1) — (0,N) CARD_rEQUEST
Association : SUBMITS
— ADMIN (1) — (0,N) CARD_rEQUEST
Association : PROCESSES
— USER (1) — (1,1) CARD
Association : OWNS
— CARD (1) — (0,N) TRANSACTION
Association : GENERATES
— DEVICE (1) — (0,N) TRANSACTION
Association : EXECUTES
— CARD_REQUEST (1) — (N) DOCUMENT
Association : CONTAINS

3.3.2 Relational model

A relational database is a collection of data items organized in formally described tables from which data can be accessed or reassembled in different ways. Relational databases consist of relations (tables) where data categories are represented by columns and each row contains a unique instance of data. Relationships between tables are established using keys and constraints, ensuring data integrity and consistency [32].

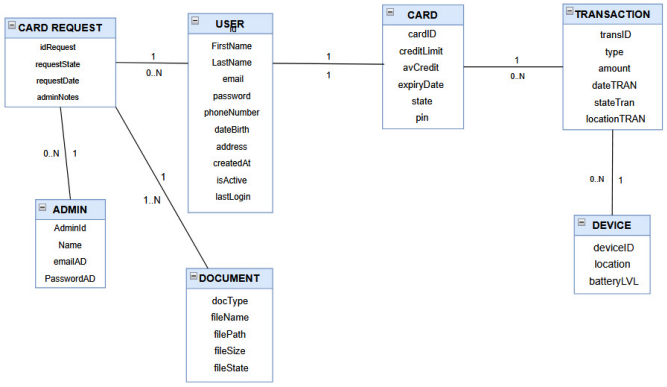


FIGURE 3.1 – Relational Model Diagram

3.3.3 Data dictionary

The data dictionary is a document that compiles all the data that will be stored in a database. It provides detailed information about each data element in the system.

ID	Signification	Size	Type	Nature	Relation
id	Unique identifier for each user	10 chars	CHAR	Element	Primary key
First_Name	first name of the user	14 chars	CHAR	Element	
Last_Name	last name of the user	14 chars	CHAR	Element	
email	email of the user	100 chars	CHAR	Element	
password	password of the admin's account	14 chars	CHAR	Element	
phone	number phone of the user	12 chars	CHAR	Element	
datebirth	birthday of the user	/	Date	Element	
Adress	adress of the user	100 chars	CHAR	Element	
createdAt	time of creation the user's acount	/	DATETIME	Element	
isactive	state of the user	/	BOOL	Element	
lastlogin	last login of the user	/	DATETIME	Element	
adminID	Unique identifier for each admin	10 chars	CHAR	Element	Primary key
emailAD	email of the Adlin	100 chars	CHAR	Element	
Name	name of the admin	14 chars	CHAR	Element	
passwordAD	password of the admin's account	14 chars	CHAR	Element	
cardid	card identifier unique for each card	20 chars	CHAR	Element	Primary key
creditlimit	limit credit of the card	3 integers	integer	Element	

TABLE 3.1 – Data dictionary(1)

ID	Signification	Size	Type	Nature	Relation
avcredit	available credit of the card	3 integers	integer	Element	
expirydate	expired date of card	/	Date	Element	
state	state of card	3 integers	integer	Element	
pin	pin of card	20 chars	CHAR	Element	
transID	transaction's identifier (unique)	10 chars	CHAR	Element	Primary key
type	transaction's type	20 chars	CHAR	Element	
amount	transaction's amount	/	float	Element	
dateTRAN	transaction's date	/	Date	Element	
stateTran	transaction's state	20 chars	CHAR	Element	
locationTRAN	transaction's location (country)	50 chars	CHAR	Element	
idrequest	request for card identifier (unique)	50 chars	CHAR	Element	Primary key
adminNotes	notes of admin about request	200 chars	CHAR	Element	
requestState	state of request	50 chars	CHAR	Element	
requestDate	Date of request	/	DATETIME	Element	
doctype	type of uploaded document	20 chars	CHAR	Element	
filename	name of uploaded document	20 chars	CHAR	Element	
filepath	path of uploaded document	100 chars	CHAR	Element	
filesize	size of uploaded document	/	float	Element	
filestate	state of uploaded document	20 chars	CHAR	Element	

TABLE 3.2 – Data dictionary(2)

deviceid	device identifier	20 chars	CHAR	Element	Primary key
location	Physical location of device	50 chars	CHAR	Element	
batteryLVL	Device battery percentage	3 integers	INTEGER	Element	

TABLE 3.3 – Data dictionary(3)

3.3.4 UML (Unified Modeling Language)

The UML is a modeling language for specifying, visualizing, constructing, and documenting the artifacts of a system intensive process.

3.3.4.1 Use case diagram definition

The use case diagram allows us to describe the possible usage scenarios (use cases) that a system is developed for. It shows what the system does and how users interact with it also it identifies the actors and the actions they can perform using the system.

Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. So when a system is analyzed to gather its functionalities use cases are prepared and actors are identified [40].

3.3.4.2 Application use case diagram

Figure presents the use case diagram of application(mobile /web). The application will provide a set of basic functionalities to interact with the tourism card system (750 Euro) to the users as well as the admin. The functionalities are :

1. **User Registration :** The application will provide a functionality to register a new account to the users.
2. **Login :** Once the account is created, users will be able to log in to the application securely.
3. **Request Tourism Card :** The users will be able to request a tourism card (750 Euro).
4. **View Card Information :** The users will view the details related to the card.
5. **View Transaction History :** He users will view all the transactions related to the card.
6. **Card Renewal :** The users will renew the tourism card when it expires.
7. **Block Card :** The users will block the card if it is lost or stolen.
8. **Change PIN Code :**The users will change the security pin code associated with the card.
9. **expiredcards :** The users will view the list of expired cards.
10. **Administrator Management :** The administrator can approve or reject card requests and manage users.

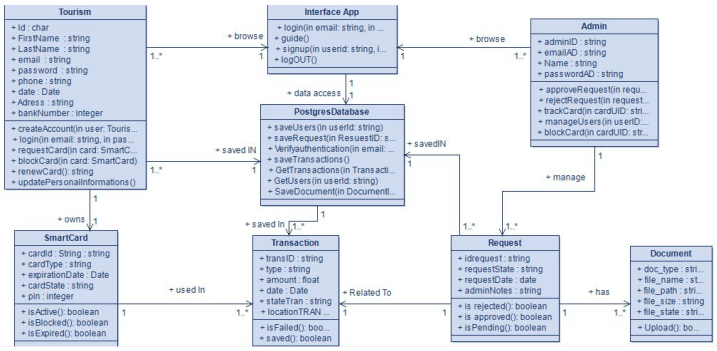


FIGURE 3.2 – Use case diagram of application

3.3.4.3 Device use case diagram

Figure presents the use case diagram of the smart card validator device. It describes how the cardholder interacts with the device to activate the card, including authentication and communication with the bank server. The diagram also shows the role of the maintenance technician, who interacts with the device to perform maintenance and ensure its proper functioning.

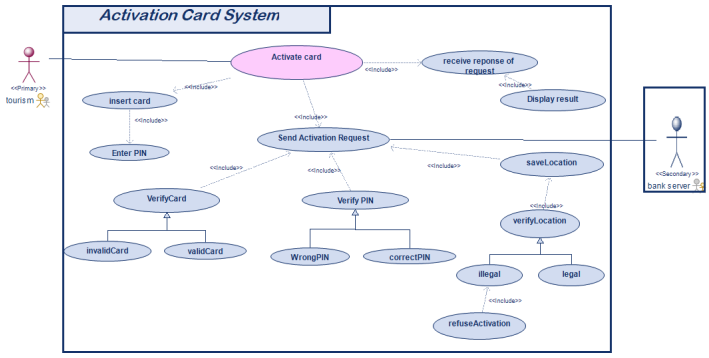


FIGURE 3.3 – Use case diagram of device

— Within a system intensive process, a method is applied as a process to derive or evolve a system.
— As a modeling language, it focuses on understanding a subject via the formulation of a model of the subject.
— As a language, it is used for communication. That is, a means to capture knowledge (semantics) about a subject and express knowledge (syntax) regarding the subject for the purpose of communication. The subject is the system under discussion.

3.3.4.4 Sequence diagram definition

Sequence Diagrams Provide detailed insights into the dynamic interactions between system components, making themessential for design, implementation, and troubleshooting phasess [33].

3.3.4.5 Application's web sequence diagram

The diagram shows the process of how the user interacts with the tourism platform. It shows all the steps that the user can perform while using the tourism platform. It

starts with the login process for the user who has already created an account. The login process verifies the account information of the user. If the login is successful, it shows the dashboard. If the login fails, it shows an error. Once the login process is successful, the user can interact with the dashboard. The dashboard sends the messages to the tourism platform and the database. The user can perform several activities on the dashboard, including seeing the card, blocking the card, renewing the card, asking for a new card, seeing the history of the card, and updating the information of the user. The diagram shows the messages exchanged between the user, the dashboard, the tourism platform, and the database lifelines. It also shows the alt fragment that shows the condition of the login process.

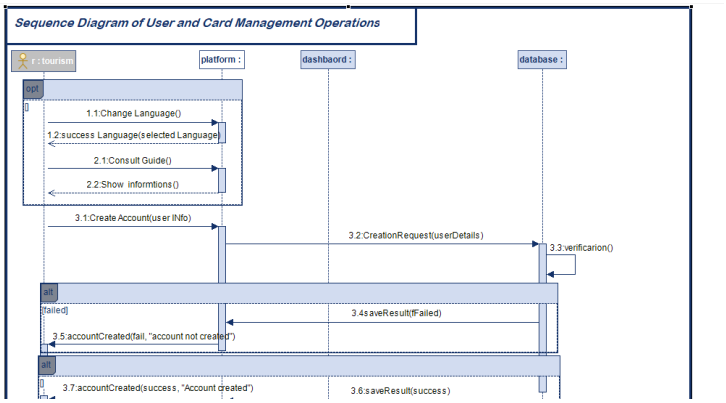


FIGURE 3.4 – Sequence diagram of application (1)

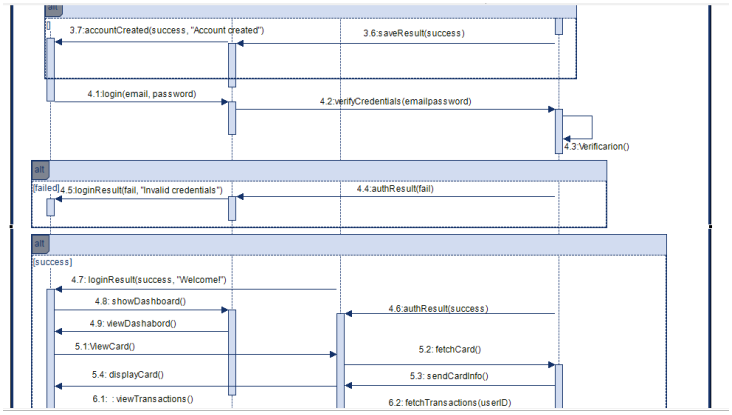


FIGURE 3.5 – Sequence diagram of application (2)

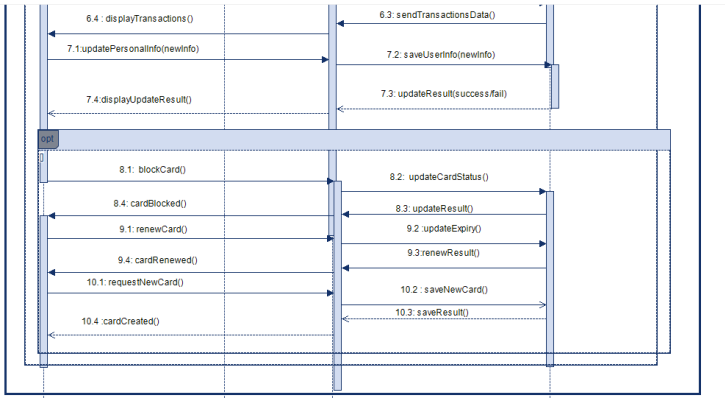


FIGURE 3.6 – Sequence diagram of application (3)

3.3.4.6 Device's sequence diagram

This diagram illustrates how the smart card validation device works, how different parts of it come together to ensure that a tourism smart card is activated. It begins with your card being tapped on the device's NFC reader ; this reads your card's identification details. This is then sent to the encryption module to ensure it is encrypted before it is passed through. Then, you enter your PIN on the device's keypad ; this is also encrypted to ensure your privacy is maintained. At the same time, your current location is obtained through the GPS module. Once all parts are in place—the card details, your PIN, and your location—the activation request is sent to the server. This is then processed by the server to ensure the card is original before the action is allowed.

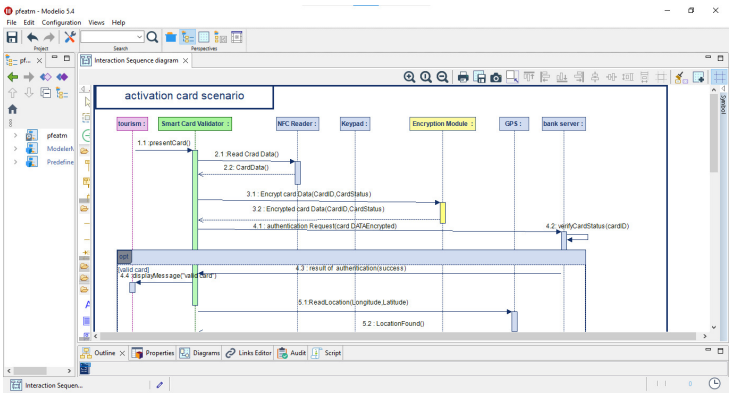


FIGURE 3.7 – Sequence diagram of device (1)

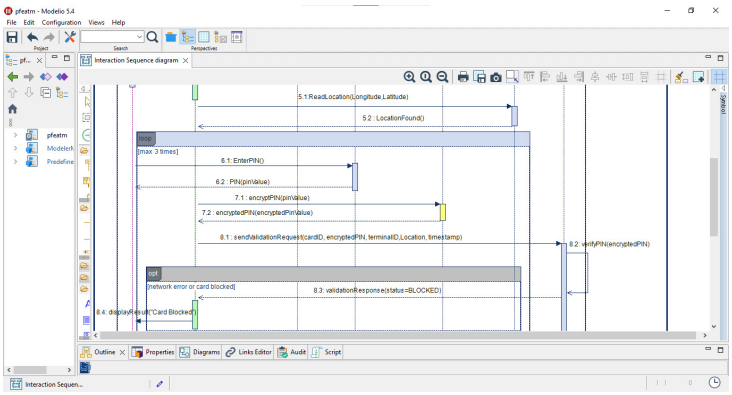


FIGURE 3.8 – Sequence diagram of device (2)

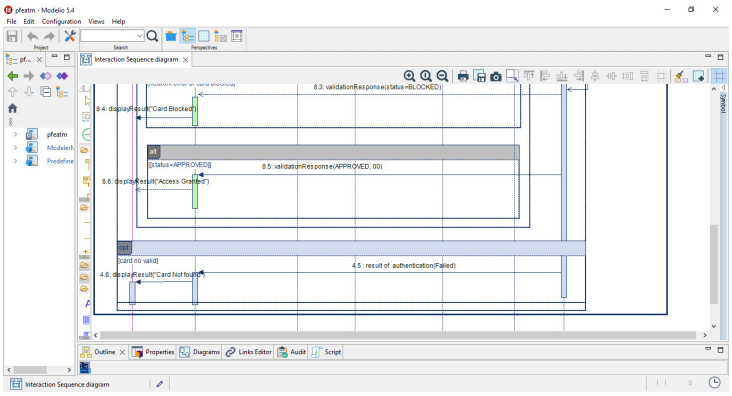


FIGURE 3.9 – Sequence diagram of device (3)

3.3.4.7 Class diagram definition

The class diagram, being the most common in modeling object-oriented systems , is used to model the static design view of a system. According to MDA , the automatic transition from class diagram into platform-specific software components is done by performing a model transformation, where model elements and parameters are mapped to corresponding elements and parameters in the software code. [43].

3.3.4.8 Device's class Diagram

The following figure describes the class diagram of our validation device.

1. **User :** have just one tourism card.
2. **Activation :** user tap his card and enter his pin for card activation.
3. The users can do more than one activation card in different periods.
4. **ATM device :** show the result or response of the bank server .
5. **Backend server :** responsible for data verification (uid of card and pin , location of device).

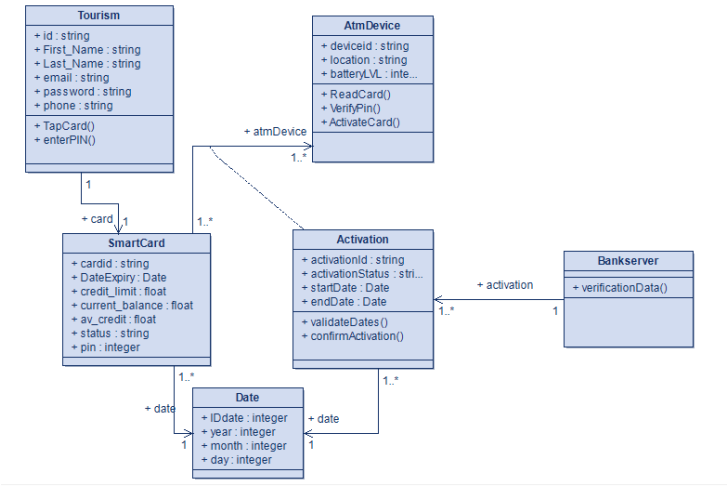


FIGURE 3.10 – Class diagram of device

3.3.4.9 Application's class Diagram

This part presents a class diagram for the Smart Tourism Card application, which shows how all the main elements work together to provide user accounts and card services. This class diagram focuses specifically on how all the main elements work together within the application to provide users with specific functionality.

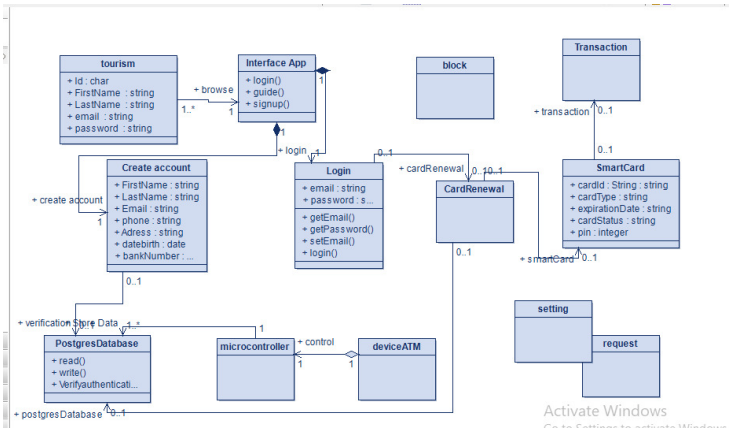


FIGURE 3.11 – Class diagram of application

3.3.4.10 Deploiment diagram definition

Deployment diagram is another type of structural UML diagram representing the hardware based upon which the software is going to run for performing some functionality. Deployment diagrams are made of different UML shapes. The 3D boxes (nodes) represent the basic hardware or software components. Lines represent the relationship between nodes and the small shapes in the boxes represent deployed artifacts.Deployment diagram shows the interaction between software and hardware to complete the functionality. Let us see an example of a deployment diagram of a web application [6].

The figure indicates the composition or the composition plan for the Smart Card Validator. For example, the deployment diagram indicates the physical composition for the Smart Card Validator.

1. The device is used to run the application for validating the smart cards.
2. The data is communicated through the Internet with the wireless connection to reach the server.
3. The data is then processed through the application services to perform the authentication for the smart cards.
4. The data is stored in the database for the users .
5. The nodes are connected to show the composition plan for the Smart Card Validator device to ensure the real-time processing for the smart card validation system.

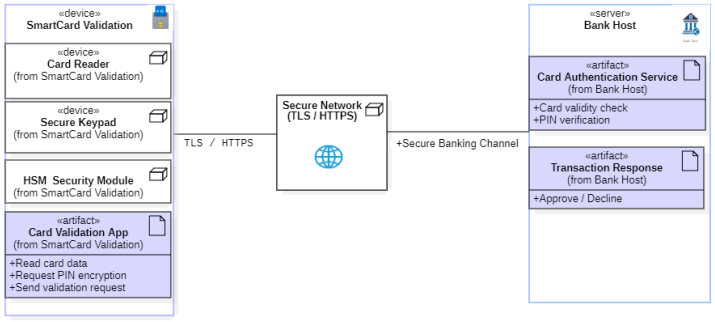


FIGURE 3.12 – Deployment diagram of device

3.4 System design

Design is an important stage in creating a project. To illustrate our work, we constructed general structures that explain it :

3.4.1 General architecture

Now we show you a simplified illustration that explains our project :

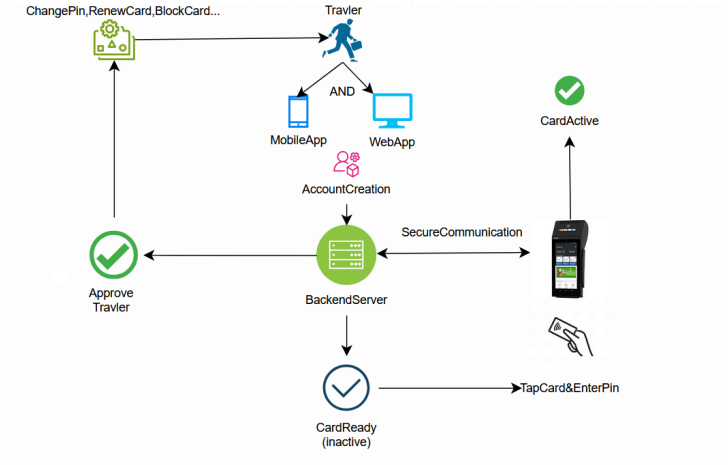


FIGURE 3.13 – General architecture of the system

3.4.2 Architecture of the card validation process

This architecture illustrates the interaction between the different hardware and software components involved in the card validation process. It shows how card data and the user PIN are captured, secured, and transmitted to the bank server for verification. The overall process ensures secure authentication and reliable authorization.

Figure below represents the detailed architecture of the card validation process.

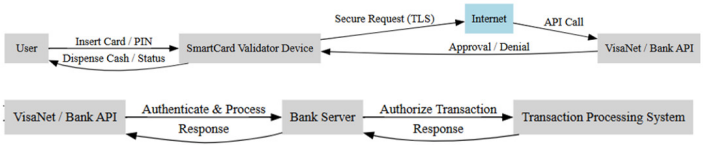


FIGURE 3.14 – Architecture of the card validation process

3.4.3 Electronic architecture

The following diagram illustrates the electronic architecture of the Smart Card Validator terminal. The system is based on an ESP32 microcontroller, which controls the device, processes data, and manages Wi-Fi communication. An RFID/NFC reader is used to read the smart card, while a secure keypad allows the user to enter the PIN. A buzzer and LED indicators provide audio and visual feedback during the activation process. A GPS module is integrated to determine the geographical location where the TourismCard is activated. The GPS communicates with the ESP32 via a serial interface and provides real-time latitude and longitude coordinates. During activation, these coordinates are sent to the backend server along with the card information to verify that the activation occurs at an authorized border point. The system is powered by a 3.7 V battery, with a voltage regulator supplying the required operating voltages to all components, as shown in Figure.

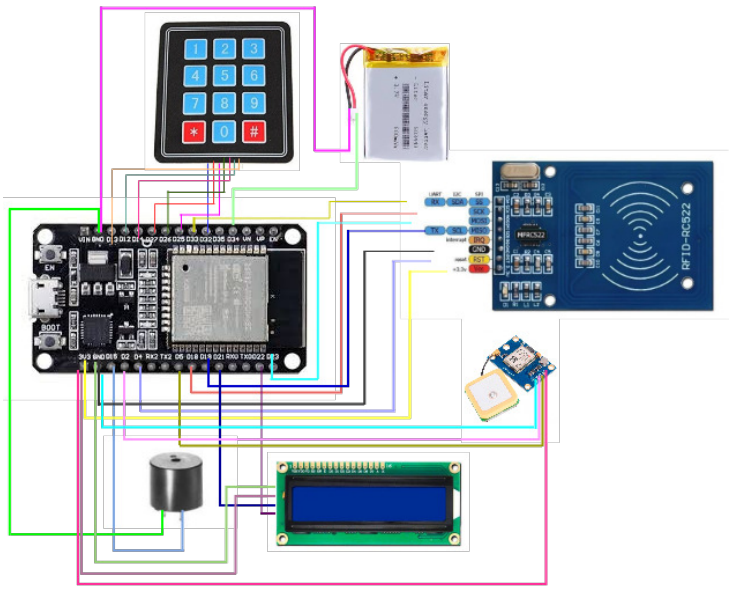


FIGURE 3.15 – Architecture of the system

3.4.4 Proposed network architecture for atm connectivity

In the future, the ATM or smart validator device will communicate with the bank servers through the telecom operator's network infrastructure. This architecture follows a hierarchical model composed of three main segments : the **Access Network**, the **Metro Network**, and the **Backbone Network**.

At the access level, the device connects to an **Optical Network Terminal (ONT)**, which acts as a fiber modem and enables communication through a **Fiber To The Home (FTTH)** connection. The data is then transmitted to the **Optical Line Terminal (OLT)** located in the operator's central office. This segment constitutes the access network that links the terminal to the telecom infrastructure.

Once the traffic reaches the OLT, it is forwarded to the **Metro Network**, where aggregation routers collect data from multiple access networks across the metropolitan area. The information is then routed through the **Backbone Network**, which provides high-speed connectivity between cities and major network facilities.

Finally, the data reaches the **bank's data center**, where security mechanisms such as firewalls protect the infrastructure and the bank servers process the transaction requests. The response is then returned to the ATM through the same communication path.

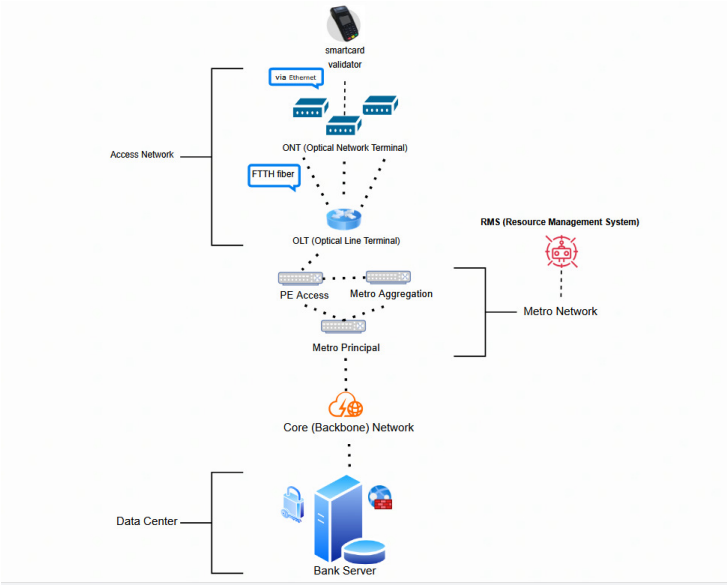


FIGURE 3.16 – Proposed telecom network architecture for ATM connectivity.

3.5 Conclusion

In this chapter, we develop a full design of the SmartCard Validator system. All the actors of the system with their functional and non-functional requirements have been identified. The system behavior was represented visually using UML diagrams, relational schema and an entity relationship diagram. Electronic architecture and network architecture illustrated the physical integration and communication processes in the system.

Chapitre 4

Implementation

4.1 Introduction

In this chapter, we present the implementation process of the proposed **SmartCard Validator System**, developed to modernize the management and activation of the Algerian tourism allowance card. The system is centered around the **Smart Tourism Card** and the **Validator Device**, which securely activates the card at airports and border points before the traveler's departure.

This chapter describes both the software and hardware implementation of the system. The software part includes a web application developed using the React framework and a mobile application developed with React Native, providing interfaces for travelers, administrators, and banking services. The hardware part focuses on the development of the SmartCard validator device using the ESP32 microcontroller and several electronic modules such as the RFID/NFC reader, keypad, LCD display, buzzer, battery, and GPS module.

We also present the programming languages, frameworks, databases, and development tools used throughout the implementation process, including PostgreSQL, Node.js, and Arduino IDE. In addition, this chapter explains the main algorithms of the system, the implemented security protocols, and the maintenance strategy adopted to ensure system reliability and scalability.

Finally, screenshots of the mobile application, web platform, and images of the developed hardware prototype are provided to illustrate the complete realization of the proposed solution.

4.2 Programming languages

There are many programming languages used in IoT, web, and mobile application development. In our project, we used several technologies to build both the software platform and the hardware prototype.

For the web application, we developed a dynamic interface for clients and administrators using the React framework, which is based on the JavaScript language.

For the mobile application, we used **React Native**, which also relies on JavaScript, to develop a cross-platform mobile app that allows users to access their accounts, manage their TourismCard, and perform actions such as requesting, blocking, or renewing the card.

For the hardware part, we used **C++** in the Arduino IDE to program the ATM device and control its components, including the NFC reader, GPS module, and network communication.

The database system is based on **PostgreSQL**, managed through the **pgAdmin 4** interface, used to store and organize users' data and transaction records. Together, these technologies form the complete implementation of our SmartCard ATM IoT system.

4.2.1 Cascading style sheets (CSS)

While HTML is used to describe the content in a web page, it is Cascading Style Sheets (CSS) that describe how that content should look. In the web design biz, the way the page looks is known as its presentation. That means fonts, colors, background images, line spacing, and page layout, all controlled with CSS. With the newest version (CSS3), you can even add special effects and basic animation to your page [45].



FIGURE 4.1 – Logo of the CSS language [46]

4.2.2 React native

React Native is used by organizations worldwide to create cross-platform phone/tablet apps with one code base. This means that you can write code easily that will run on iPhones, iPads, and Android phones and tablets without having to rewrite it in two or more languages - just one. [41].



FIGURE 4.2 – Logo of the React Native [49]

4.2.3 React

React is a JavaScript framework. React was originally created by engineers at Facebook to solve the challenges involved when developing complex user interfaces with datasets that change over time. this is not a trivial undertaking and must not only be maintainable, but also scalable to work at the scale of Facebook. React was actually born in Facebook's ads organization, where they had been utilizing a traditional client-side Model-View-Controller approach [26].

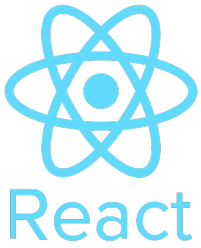


FIGURE 4.3 – Logo of the react framework [19]

4.2.4 C++

C++ is a general purpose programming language designed to make programming more enjoy-able for the serious programmer. except for minor details, C++ is a superset of the C language. C++ was designed to be a better C.support data abstraction.support object-oriented programming. [51].



FIGURE 4.4 – Logo of the C++ programming language [15]

4.3 Development tools and frameworks

In this section, we present the tools and frameworks used in implementing our project.

4.3.1 PgAdmin database

pgAdmin is generally used as the graphic user interface (GUI) management tool for PostgreSQL and installed by default with new installations. Prior to 2018, if a user executed a query on geographic objects, the user would need to use an external application, such as QGIS or OpenJump to view the resulting geometries. pgAdmin4 was released in mid- 2016 as a web-based application written in Python and jQuery with Bootstrap, using the Flask framework. this new architecture of pgAdmin4 provided an excellent opportunity to integrate a geometry viewer into the application. After the launch of pgAdmin4, an enhancement ticket for a geometry viewer was created, however, there was no progress on this ticket until the 2018 GSoC programme. In 2018, a geometry viewer for pgAdmin4 was developed as part of the 2018 Google Summer of Code (GSoC) [28].



FIGURE 4.5 – Logo of pgAdmin [20]

4.3.2 Arduino ide

Arduino IDE is an open source software that is mainly used for writing and compiling the code into the Arduino Module [25].We will define it in points :

1. It is an official Arduino software, making code compilation too easy that even a common person with no prior technical knowledge can get their feet wet with the learning process.
2. It is easily available for operating systems like MAC, Windows, Linux and runs on the Java Platform that comes with inbuilt functions and commands that play a vital role for debugging, editing and compiling the code in the environment.
3. A range of Arduino modules available including Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Micro and many more.
4. Each of them contains a microcontroller on the board that is actually programmed and accepts the information in the form of code.
5. The main code, also known as a sketch, created on the IDE platform will ultimately generate a Hex File which is then transferred and uploaded in the controller on the board.
6. The IDE environment mainly contains two basic parts : Editor and Compiler where former is used for writing the required code and later is used for compiling and uploading the code into the given Arduino Module.
7. This environment supports both C and C++ languages.



FIGURE 4.6 – Logo of Arduino IDE [21]

4.3.3 Node.js

Node.js (Node) is a cross platform runtime environment originally developed in 2009 by Ryan Dahl for developing server-side applications. it can be regarded as server-side JavaScript. It was created to address the issues platforms can have with the performance

in network communication time dedicating excessive time processing web requests and responses.

Node.js is a platform built on Chrome's JavaScript runtime for easily building fast, scalable network applications. Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient, perfect for data-intensive real-time applications that run across distributed devices . [10]



FIGURE 4.7 – Logo of Node.js [17]

4.4 The electronic equipment.

In this section, we will describe the electronic devices used in our project.

4.4.1 ESP32 microcontroller

ESP32 is a powerful SoC (System on Chip) microcontroller with integrated Wi-Fi 802.11 b/g/n, dual-mode Bluetooth version 4.2, and a variety of peripherals. It is an advanced successor of the 8266 chip, primarily in the implementation of two cores clocked in different versions up to 240 MHz. compared to its predecessor, except these features, it also extends the number of GPIO pins from 17 to 36, the number of PWM channels per 16, and is equipped with 4 MB of flash memory [3].



FIGURE 4.8 – Model ESP32 [22]

4.4.2 Keypad (matrix 3*4)

Keypads play important role in a small embedded system where human interaction or human input is needed. All we have to do is connect the rows and columns to a port of microcontroller and program the controller to read the input. We make the rows as i/p and we drive the columns making them o/p, this whole procedure of reading the keyboard is called scanning. A 3 x 4 matrix keypad is used for data entry. The 12 push switches are connected to seven lines of port A [7].



FIGURE 4.9 – Keypad(3*4) [39]

4.4.3 NFC/RFID reader

Near Field Communication (NFC) is a technology that allows two devices to exchange information wirelessly at close range. more precisely, NFC is a set of technical specifications and standards for transferring information between two proximate objects via the inductive coupling of radio frequency fields at 13.56 MHz. NFC evolved out of existing radio-frequency identification (RFID) standards, already familiar to many librarians, such that NFC-enabled devices can be compatible with some existing RFID systems and infrastructure [38].

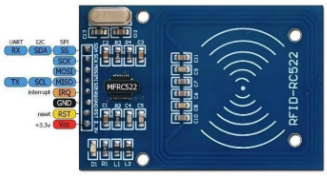


FIGURE 4.10 – NFC/RFID reader [37]

4.4.4 Active buzzer

Electrical oscillations are transformed into sound vibrations by the buzzer. the operation and function of a buzzer are similar to those of a loudspeaker, nevertheless, they are simpler to use. the buzzer can be used as an indicator or a transducer (it has a built-in driver circuit but no driver circuit itself). when operating, a buzzer intended as a transducer needs an input voltage in the form of a square wave with a specific frequency, whereas a buzzer designed as an indicator merely needs a constant DC voltage or current source. while indicator buzzers and transducer buzzers can both be operated to produce a continuous tone or sound in the form of fast or slow pulses, only transducer buzzers are capable of producing noises with high or low tones, sirens, or specific melodies [30].



FIGURE 4.11 – Active buzzer [30]

4.4.5 Display 16*2 HD 44780

Liquid Crystal Display works like a simplified computer monitor which facilitates human–machine interaction and provides the users with feedback and status updates or real-time data as the sensors collect information [36].

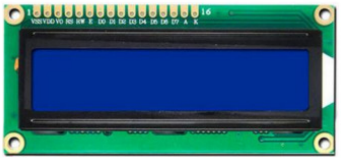


FIGURE 4.12 – Display 16*2 HD 44780 [39]

4.4.6 3.7V battery



FIGURE 4.13 – 3.7V battery

4.4.7 GT-U7 GPS module

Our device can use a GPS module to retrieve their position in real-time. The module used is the GT-U7 by Goouuu Tech, assembled into a circuit board by MakerHawk . This module takes 3.3V as input voltage. It uses the UART protocol to communicate with the MCU, and thus necessitates two connections : the Rx pin of the module must be connected to a serial Tx pin of the MCU, and vice-versa. It can measure, among others, the latitude, longitude, and altitude, when a GPS signal is found [18].



FIGURE 4.14 – GT-U7 GPS module [18]

4.5 The main algorithms of the system

Here we will introduce the main algorithms that we have developed in our project .

4.5.1 Pseudo algorithms on the application side

4.5.1.1 Pseudo-algorithm for request new Card

This algorithm allows the **traveler** to **request a new tourism card**. firstly checks if the **user exists** and does not already have a **pending request**. After that, it verifies that all **required documents** are **provided and valid**. Then, the system **saves the documents**, **creates a new request**, and **notifies the user** by **email and SMS**.

Algorithm 1 Request new card

```
1: Begin
2: Input : userID, documents (First Page of Passport,Land Travel Receipt, Valid
   Visa,Family Record.....)
3:
4: // Check if user exists
5: user = findUserByID(userID)
6: if user not found then
7:     return error "User not found"
8: end if
9:
10: // Check for existing pending request
11: pending = checkPendingRequest(userID)
12: if pending exists then
13:     return error "You already have a pending request"
14: end if
15:
16: // Validate documents
17: if missing documents then
18:     return error "All documents required"
19: end if
20:
21: // Save documents to storage
22: saveDocuments(userID, documents)
23:
24: // Create request record
25: requestID = generateID()
26: saveRequest(requestID, userID, "pending",documents)
27:
28: // Notify user
29: sendEmail(user.email, "Card request received")
30: sendSMS(user.phone, "Your card request is being processed")
31:
32: return success "Request submitted. Processing time : 2-3 days"
33: End
```

4.5.1.2 Pseudo-algorithm for request processing (Admin)

This algorithm is used by the **admin** to **process card requests sended bu traveler**. If the request is **approved**, the system **generates the card details** (**number, PIN, expiry date**) and **notifies the user**. If **rejected**, the system **updates the request status** and **sends the reason to the user**.

Algorithm 2 Verify card request

```
1: Begin
2: Input : adminID, requestID, decision, comments
3:
4: // Get request
5: request = findRequestByID(requestID)
6: if request not found then
7:     return error "Request not found"
8: end if
9:
10: // Get user
11: user = findUserByID(request.userID)
12:
13: if decision = "approve" then
14:     // Generate card details
15:     cardNumber = generateCardNumber()
16:     pin = generatePIN()
17:     expiry = calculateExpiryDate(5 years)
18:
19:     // Create card
20:     cardID = generateID()
21:     saveCard(cardID, user.id, cardNumber, pin, expiry, "inactive")
22:
23:     // Update request
24:     updateRequestStatus(requestID, "approved", cardID)
25:
26:     // Notify user
27:     sendEmail(user.email, "Card approved - waiting for activation")
28:     sendSMS(user.phone, "Your card has been approved")
29: else if decision = "reject" then
30:     updateRequestStatus(requestID, "rejected", comments)
31:     sendEmail(user.email, "Card request rejected : " + comments)
32: end if
33:
34: return success
35: End
```

4.5.1.3 Pseudo-algorithm of card renewal

This algorithm allows a **traveler** to **renew their tourism card** if it is **expired**.

Algorithm 3 Renew card

```
1: Begin
2: Input : userID, cardID
3: card = findCardByID(cardID)
4: if card not found or card.userID != userID then
5:     return error "Card not found"
6: end if
7:
8: if card.status != "active" and card.status != "expired" then
9:     return error "Card cannot be renewed"
10: end if
11:
12: existing = findPendingRenewal(cardID)
13: if existing exists then
14:     return error "Renewal already in progress"
15: end if
16:
17: // Generate new card with same number but new expiry
18: newExpiry = calculateExpiryDate(1 years)
19: // Create new card id (replaces old one)
20: newCardID = generateID()
21: saveCard(newCardID, userID, card.cardNumber, card.pin, newExpiry, "inactive")
22:
23: // Link to old card
24: setReplacementCard(cardID, newCardID)
25:
26: updateCardStatus(cardID, "replaced")
27:
28: // Create renewal record
29: renewalID = generateID()
30: saveRenewal(renewalID, cardID, newCardID, userID, "pending")
31:
32: user = findUserByID(userID)
33: sendEmail(user.email, "Your renewed card has been ordered")
34: sendSMS(user.phone, "Your new card will arrive in 3-5 days")
35:
36: return success "Renewal initiated. New card will be delivered soon."
37: End
```

4.5.1.4 Pseudo-algorithm of card blocking

Card blocking

This algorithm is used to **block a card** in case of **loss**, **theft**, or **suspicious activity**. It **verifies the card**, **updates its status to "blocked"**, **saves the reason**, and **notifies the user** via **email**, **WhatsApp**, and **account notification**.

Algorithm 4 Block Card

```
Begin
Input : userID, cardID, reason (lost/stolen/suspicious)

card = findCardByID(cardID)
if card not found or card.userID != userID then
    return error "Card not found"
end if

if card.status = "blocked" then
    return error "Card already blocked"
end if

// Block the card
updateCardStatus(cardID, "blocked")

// Save block reason
saveBlockRecord(cardID, userID, reason)


sendSMS(user.phone, "Your card has been blocked. " + message)
sendEmail(user.email, "Card blocked - " + reason)

End
```

4.5.1.5 Pseudo-algorithm of change PIN of card(admin side)

This algorithm designed to **change the card PIN**. It **checks if the new PIN is valid**, **verifies the old PIN**, and **updates it**. If successful, the user **receives a confirmation message**.

Algorithm 5 Change PIN

```
Begin
Input : userID, cardID, oldPIN, newPIN

// Validate new PIN
if length(newPIN) != 4 or not numeric(newPIN) then
    return error "PIN must be 4 digits"
end if

// Find card
card = findCardByID(cardID)
if card not found or card.userID != userID then
    return error "Card not found"
end if

// Check if card is active
if card.status != "active" then
    return error "Card must be active"
end if

// Verify old PIN
if not verifyPIN(card.pin, oldPIN) then
    FailedAttempts(cardID)
    return error "Incorrect PIN"
end if

// Save new PIN
updateCardPIN(cardID, newPIN)

// Notify user
sendSMS(user.phone, "Your PIN has been changed")

return success "PIN changed successfully"
End
```

4.5.2 Pseudo algorithms on the device side

4.5.2.1 Pseudo-algorithm for RFID card detection

This Pseudo-algorithm **detects when a card is placed** near the **RFID reader**. Once detected, it **reads the card UID**, **displays a message** on the screen, and then **asks the user to enter the PIN**.

Algorithm 6 RFID Card Detection

```
1: Begin
2: Initialize RFID reader
3: while device is ON do
4:     if new card is present then
5:         Read card UID
6:         if UID exist then
7:             Save current UID
8:             Set cardScanned = true
9:             Display "CARD DETECTED" with UID on LCD
10:            Wait 1.5 seconds
11:            Call PINEntryProcedure()
12:        end if
13:        Halt card communication
14:    end if
15: end while
16: End
```

4.5.2.2 Pseudo-algorithm for card activation

This Pseudo-algorithm **activates a card** using the **entered PIN**. It **sends the card information to the server** and **waits for a response**. If successful, the card is **activated**; otherwise, an **error message is displayed**.

Algorithm 7 Card Activation

```
1: Begin function activateCard()
2: // Prepare activation request
3: jsonData = {
4:     card_uid : currentUID,
5:     pin : enteredPIN
6: }
7: Send POST to "/api/activate-card"
8: if HTTP response code == 200 then
9:     Parse JSON response
10:    if was_activated == true then
11:        Save transaction : "Card activated"
12:        Display "CARD ACTIVATED SUCCESS!"
13:    else
14:        if response contains "expired" then
15:            Display "CARD EXPIRED"
16:        else if response contains "already active" then
17:            Display "CARD ALREADY ACTIVE"
18:        else
19:            Display "ACTIVATION FAILED"
20:        end if
21:        Play wrong PIN beep
22:        Delay 3 seconds
23:    end if
24: else
25:    Display "SERVER ERROR"
26:    Play wrong PIN beep
27: end if
28: End function
```

4.5.2.3 Pseudo-algorithm for GPS location tracking

This algorithm **continuously tracks the device location** using **GPS**. When a **new location is available**, it **sends the coordinates to the server** via **WiFi**. If there is **no connection**, the data is **saved locally**.

Algorithm 8 GPS Location Tracking

```
Begin
Initialize GPS serial communication
while device is ON do
    while GPS data is available do
        Read GPS character
        Feed to GPS parser
    end while
    if GPS location is updated then
        latitude = get latitude from GPS
        longitude = get longitude from GPS
        Call sendLocationToServer(latitude, longitude)
    end if
end while
End

Function sendLocationToServer(latitude, longitude)
if WiFi is connected then
    jsonData = {
        card_uid : currentUID,
        latitude : lat itude,
        longitude : longitude
    }
    Send POST to "/api/gps-location"
    if HTTP request successful then
        Log "GPS sent successfully"
    else
        Log "GPS send error"
    end if
else
    Log "No WiFi - GPS saved locally"
end if
End function
```

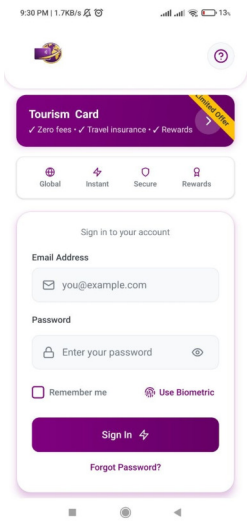
4.6 Mobile application

The mobile-responsive application serves as the tourist's personal management hub for the tourism smart card ecosystem. Accessible via any smartphone, tablet, this secure portal gives travelers direct control over their card and spending, removing dependency on physical service points for routine tasks.

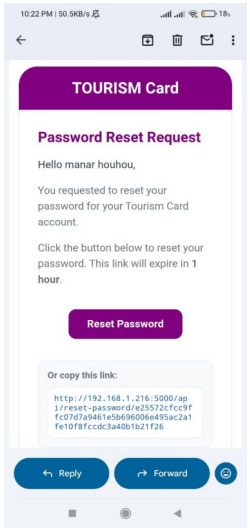
4.6.1 Login page

This page allows the user to log in to their account on our Tourism card application As shown in the picture below , this login page include guide for users.

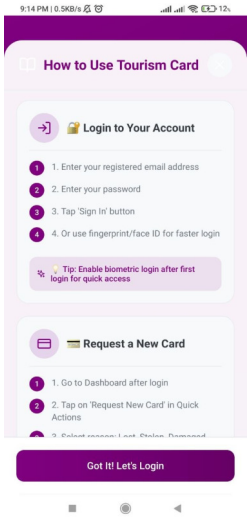
The page also offers a user manual that helps users to navigate the application. The user manual provides information on the procedures to follow when creating an account for users who do not have one, the requirements of the password, and the procedures to follow when recovering the password through the "Forgot Password" link provided on the page. In addition, the page offers contact information to aid users who need further assistanceas showing in figure.



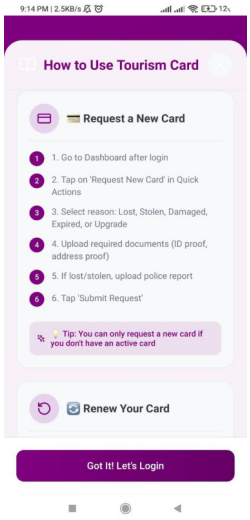
Login Page



Forget password page



Guide page 1



Guide page 2

FIGURE 4.15 – Authentication and guide pages

4.6.2 Dashboard page

4.6.2.1 Overview

The Dashboard Page serves as the **primary dashboard and command center** for the traveler. It is the first screen encountered after login, designed to deliver the most critical information at a glance and provide immediate access to high-priority card management functions. This page prioritizes **clarity, speed, and actionability**, ensuring users can manage their tourism finances efficiently with minimal effort.

4.6.2.2 Core Layout and Components

— **Visual Card Representation** : A prominent visual mockup of the user's **Tourism Smart Card** with a masked card number for security purposes.

— **Balance Display** : Large, clear numerical display of the **current available balance** in the local currency.
— **Status Indicators** : Color-coded indicators showing the card's operational state :
  — **Active** : Card is ready for use.
  — **Nearly Empty** : Low balance warning (ex : below 20% of initial load).
  — **Blocked** (Red) : Card has been frozen for security reasons.

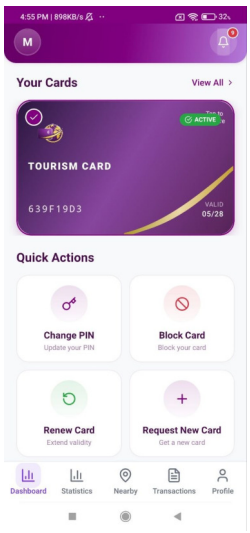


FIGURE 4.16 – Dashbaord page (01)

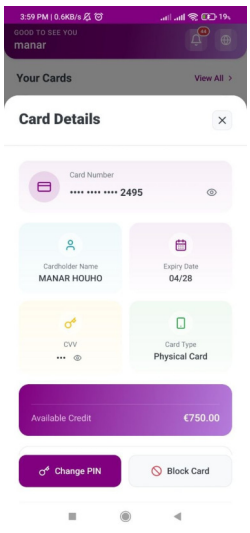


FIGURE 4.17 – Dashbaord page (02)

4.6.2.3 Quick action tray

— **Key Functions** :

1. **Renew** : Renew the tourism card if expired .
2. **Block card** : One-touch emergency button that instantly frNewes the card if lost or stolen, triggeringa requestd seca newttourism card.
3. **Change pin** : Allows the user to set a new Personal Identification Number for card security, requiring current PIN verification.
4. **View details** : Navigates to a comprehensive card information page showing full card number, expiry date, and usage limits.
5. **Request for new tourism card** : Allows the user to send request for new Tourism Card if broken or stolen.

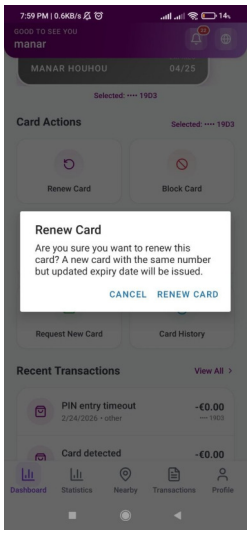


FIGURE 4.18 – Renew card section (Dashboard Page)

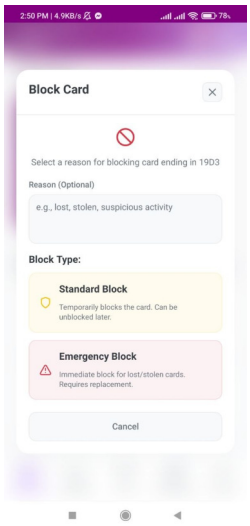


FIGURE 4.19 – Block card section (Dashboard page)

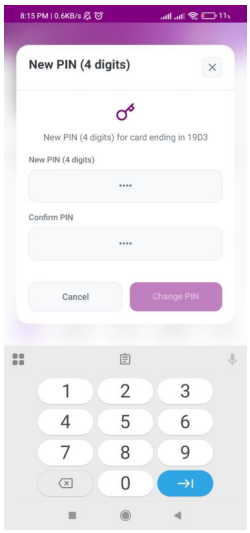


FIGURE 4.20 – Change PIN of card step (1)

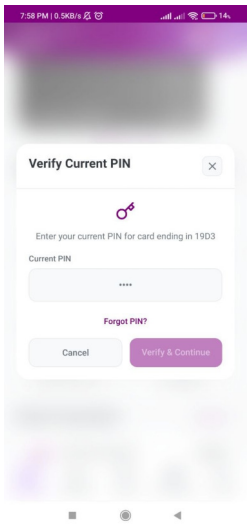


FIGURE 4.21 – Change PIN of card step (2)

FIGURE 4.22 – Card management features in dashboard

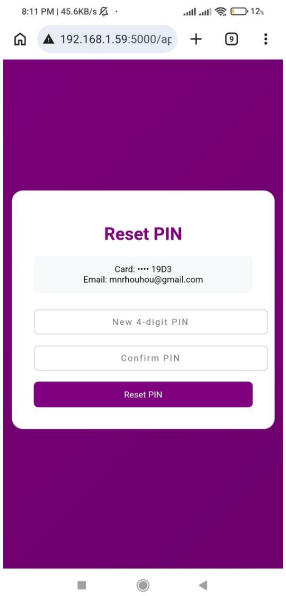


FIGURE 4.23 – Forget PIN of card (1)

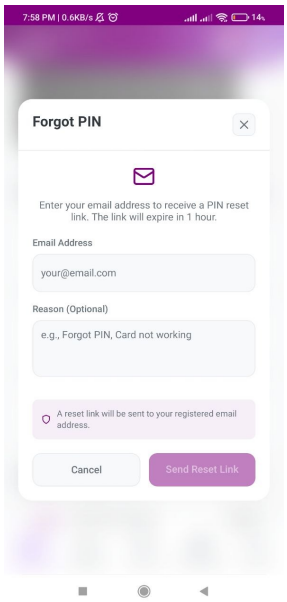


FIGURE 4.24 – Forget PIN of card (2)

4.6.2.4 Contextual alerts & notifications

— **Alert banner** : A dedicated notification area at the top of the screen that appears conditionally based on system events.
— **Alert types** :
  — Warning alert : "Low Balance : Please top-up to continue seamless payments." (Triggers when balance falls below a configurable threshold).
  — Success alert : "Your card was successfully renewed." (Appears for 5 seconds after successful renew).
  — Security alert : "Unusual activity detected."
— **Automatic email notification** :

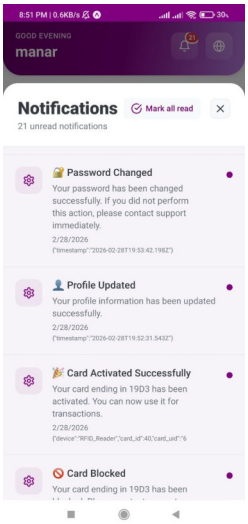


FIGURE 4.25 – Alert types

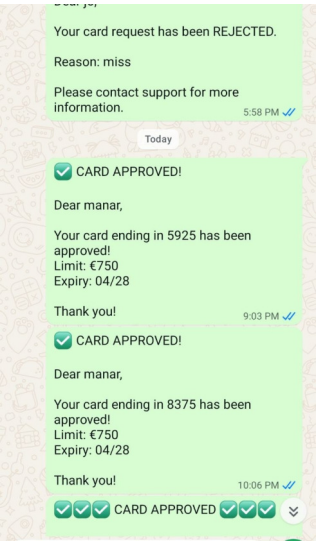


FIGURE 4.26 – WhatsApp notification

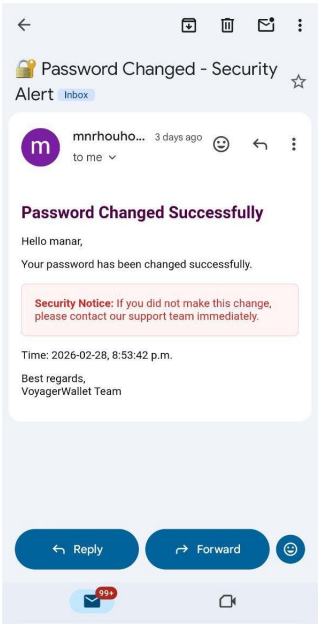


FIGURE 4.27 – Email notification (1)

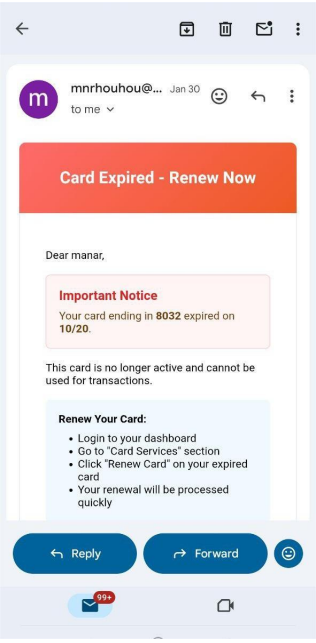


FIGURE 4.28 – Email notification (2)

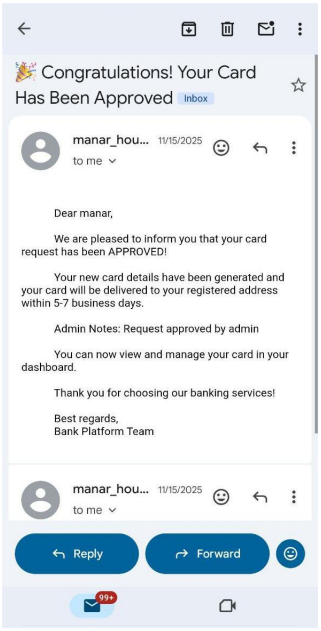


FIGURE 4.29 – Email notification (3)

FIGURE 4.30 – Notification system

4.6.3 Transactions page

The Transactions Page is the traveler's dedicated financial ledger within the mobile portal. It provides a clear, chronological, and searchable record of all spending activity linked to their Tourism Smart Card, offering full transparency and empowering users to track their travel budget with precision.As shown in the picture below.

— **Search transactions** : The user will be allowed to search for a particular transaction.
— **Download PDF** : The user will be provided with an option to download all transactions in PDF format.
— **Summarize transactions** : The user will be provided with an option to view a summary of all transactions.
— **Filter options** : The user will be provided with an option to filter the transactions based on date range, and transaction .

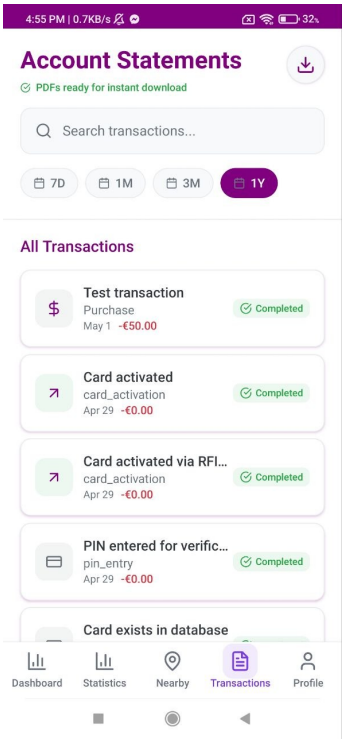


FIGURE 4.31 – Transaction page

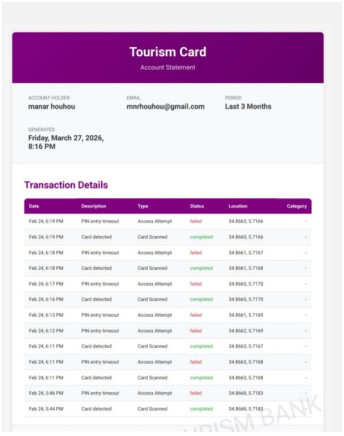


FIGURE 4.32 – Transactions file downloaded

4.6.4 Location page

The location Page functions as a real-time financial service finder within the tourism ecosystem. Moving beyond simple location display, enabling travelers to easily locate nearby facilities for Banks, Atms,and emergency services.

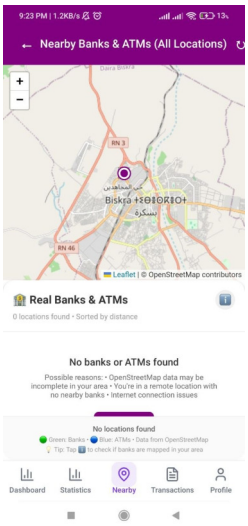
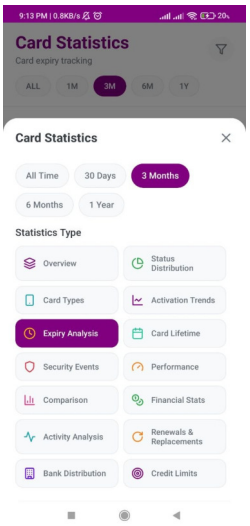


FIGURE 4.33 – Location Page

4.6.5 Statistics page

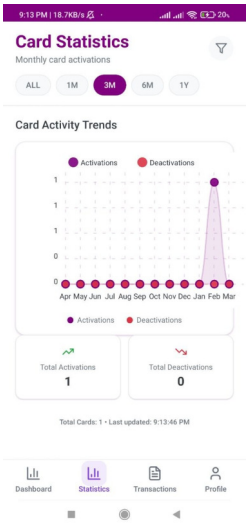
The Account Statement page displays the main statistics and card health exemple :expired date of card, Below are the main statistics displayed :



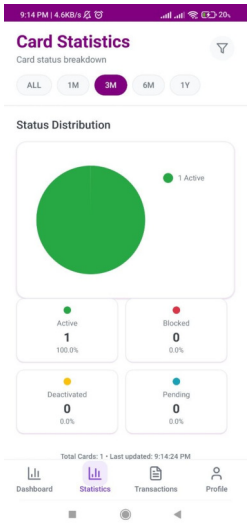
Statistics page - overview



Statistics page 1



Statistics page 2



Statistics page

FIGURE 4.34 – Statistics page views

4.6.6 Profile page

The profile page serves as the personalized user center within the mobile application, providing a secure space where the traveler can manage their identity, account settings, and control data privacy. In addition, an integrated AI chatbot assistant has been implemented to answer tourism-related questions, provide travel guidance, and assist users in obtaining quick information about tourist attractions. The AI chatbot operates using vector-based representations and weighted data processing techniques to enhance semantic understanding, recommendation accuracy, and intelligent interaction with users. As shown in the figures below.

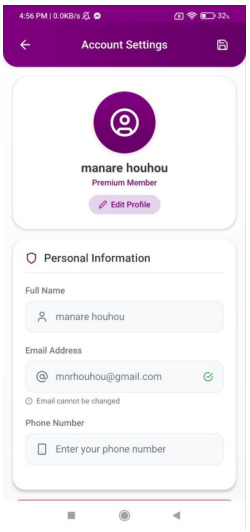


FIGURE 4.35 – Profile page (1)

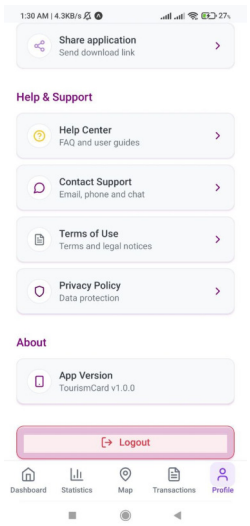


FIGURE 4.36 – Profile page (2)

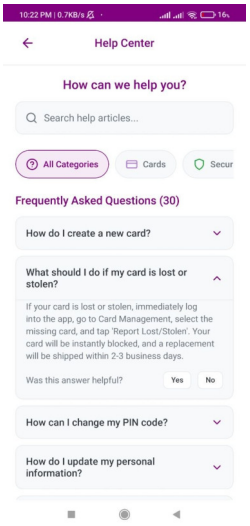


FIGURE 4.37 – Help center section

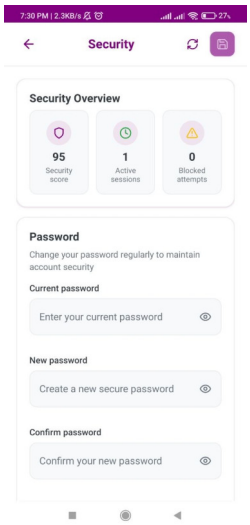


FIGURE 4.38 – Security section

FIGURE 4.39 – Profile and settings sections

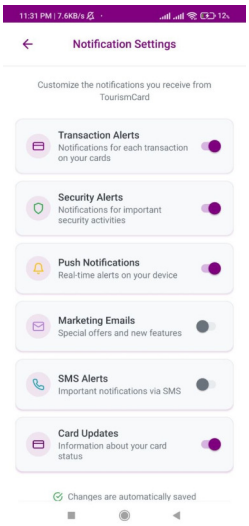


FIGURE 4.40 – Notifications setting section

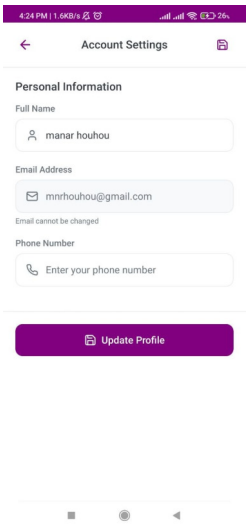


FIGURE 4.41 – General setting section

FIGURE 4.42 – Settings sections

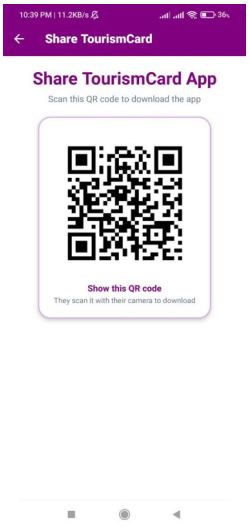


FIGURE 4.43 – QR code of application

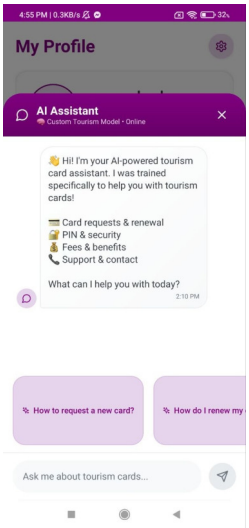


FIGURE 4.44 – IA chatbot assistance

FIGURE 4.45 – Settings Sections

4.7 Web application

The web application serves as the **centralized digital platform** for the Tourism Smart Card system, providing both travelers and administrators with secure, accessible interfaces. Accessible via any modern web browser on desktops, tablets, or smartphones, this cloud-hosted solution bridges the physical smart card infrastructure with digital convenience.

4.7.1 Home page

The Home Page is the main entry point of the web platform, providing information on the overall system while allowing the user to quickly access the main services offered. After the successful login process, the user is redirected to the personalized dashboard.

The Home page is important for the user's navigation of the platform while allowing for quick access to the services offered.

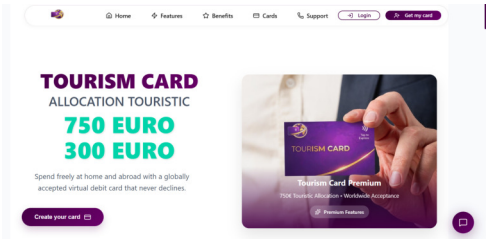


FIGURE 4.46 – Home page (1)

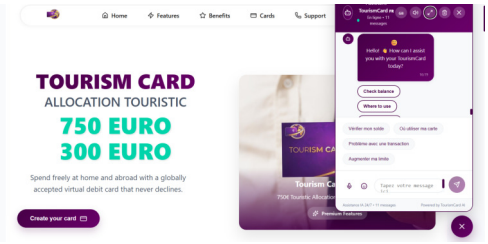


FIGURE 4.47 – Home page (2)

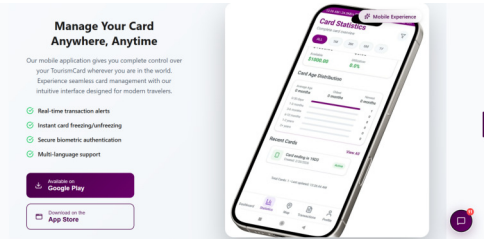


FIGURE 4.48 – Home page (3)

4.7.2 Sign in / Sign up page

This page enables users(travelers) to create a new account or access their existing account on the web platform. This is done to ensure secure authentication and protect user data by encrypting communication.

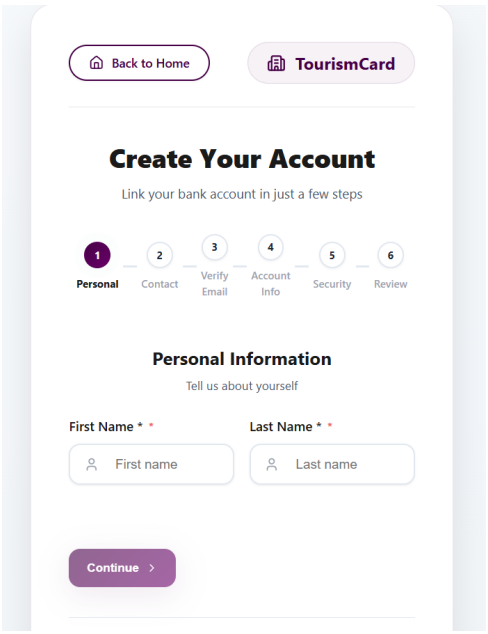


FIGURE 4.49 – Account creation

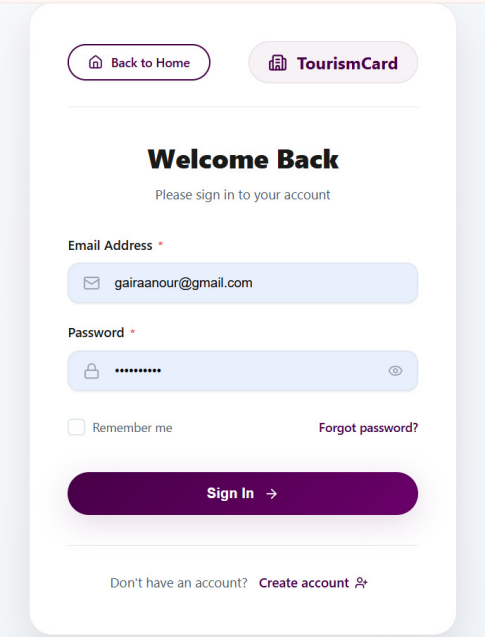


FIGURE 4.50 – Login page

4.7.3 Tourism dashbaord page

4.7.3.1 Cards management section

The topic of this section is the management of smart card, along with their state, which includes different features to enable the secure management of the card by users as well as administrators.

— **Card status control** : block the card.
— **Card renewal** : Renew expired or soon-to-expire cards.
— **PIN management** : Change or reset the card PIN securely.
— **Card details** : View card number (masked), expiry date, and usage limits.
— **Request new tourism card** : Request for new Tourism Card for the first Time.

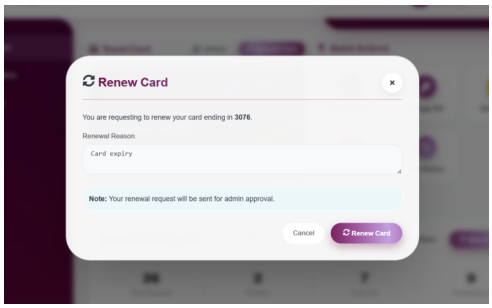


FIGURE 4.51 – Renew card section (dashbaord page)

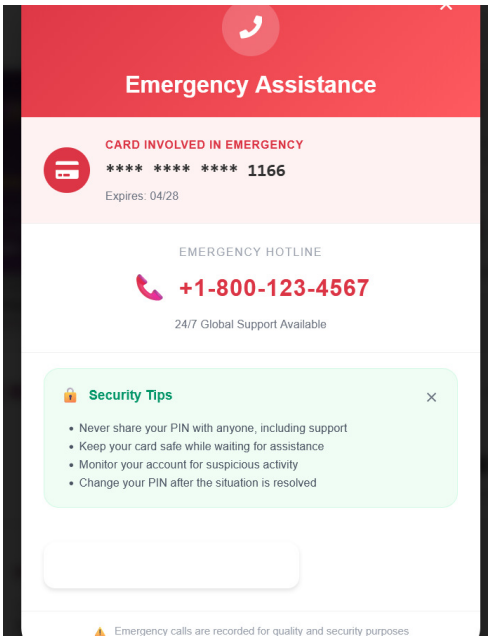


FIGURE 4.52 – Block card section (dashbaord page)

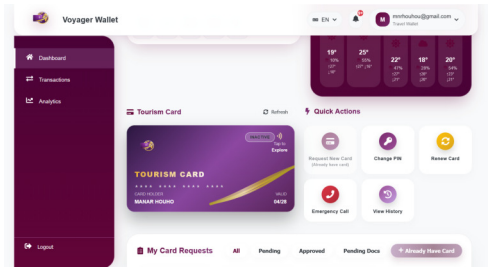


FIGURE 4.53 – View details section (dashbaord page)

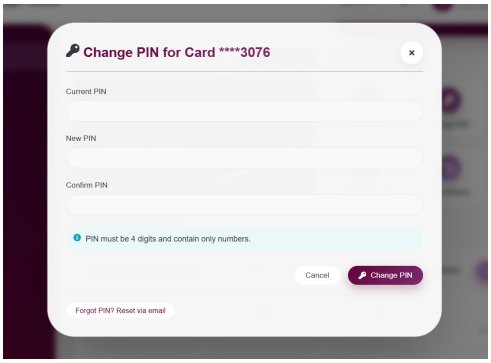


FIGURE 4.54 – Change pin of card section (dashbaord page)

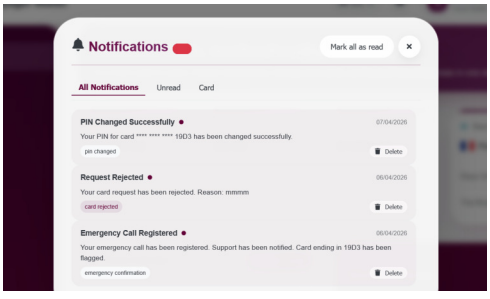


FIGURE 4.55 – Notifications section (dashbaord page)

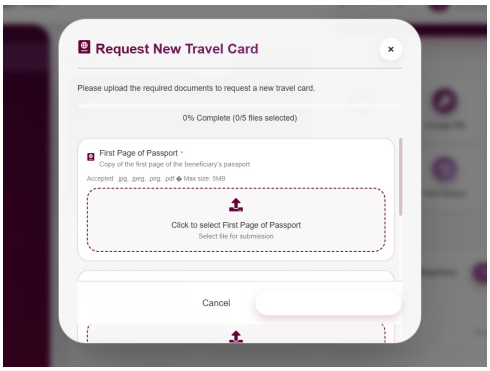


FIGURE 4.56 – Request for new tourism card

4.7.4 Transaction management page

The transaction management page allows the user to monitor all financial/operational transactions carried out using the Tourism Smart Card.

— **Search transactions** : The user will be allowed to search for a particular transaction.

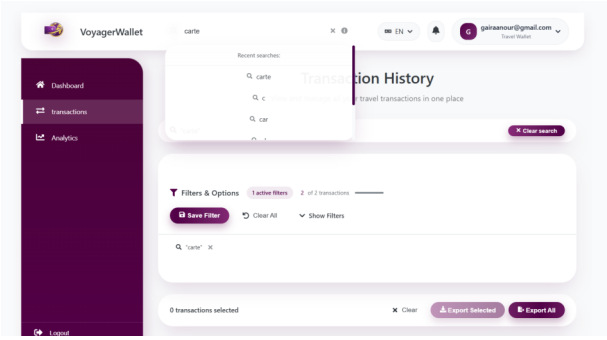


FIGURE 4.57 – Search transactions page

— **Download PDF/CSV** : The user will be provided with an option to download all transactions in PDF/CSV format.

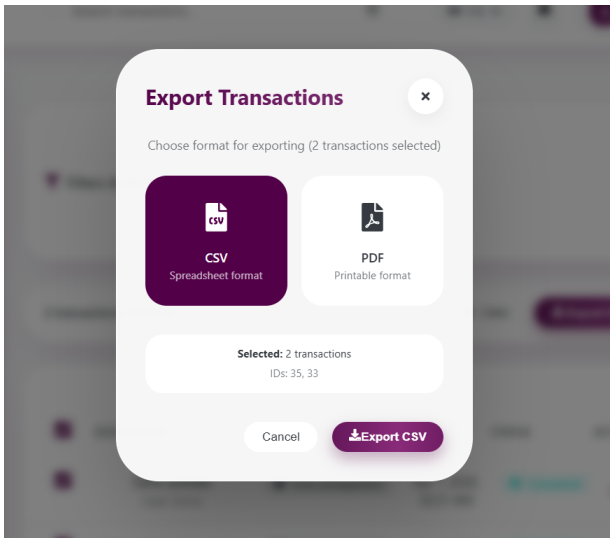


FIGURE 4.58 – Download PDF/CSV section

— **Filter options** : The user will be provided with an option to filter the transactions based on date range, and state.

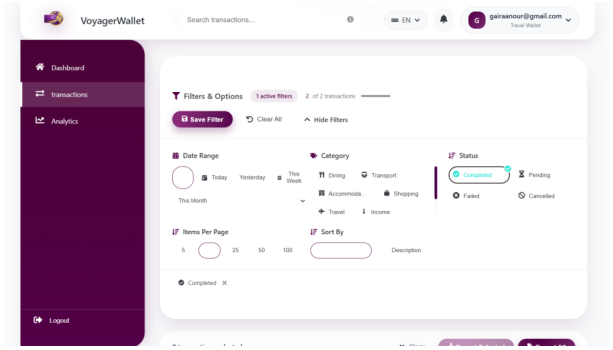


FIGURE 4.59 – Filter options section

— **Details of transactions** : The user can see details of the transactions.

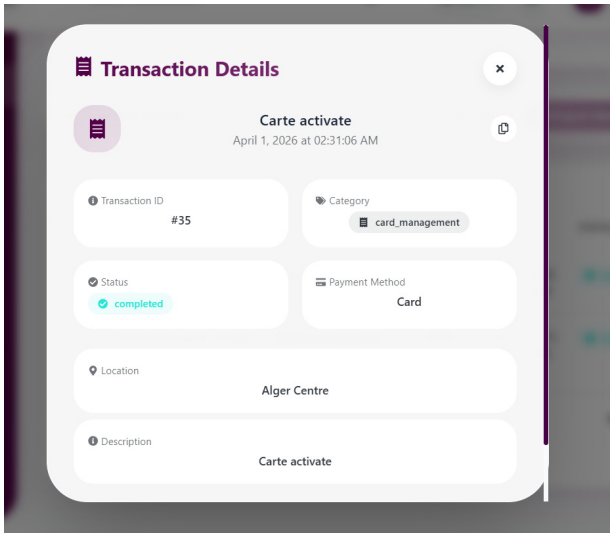


FIGURE 4.60 – Transactions details section

— **Report issue of transaction** : The user can Report an Issue with transaction if any problem about this Transaction.

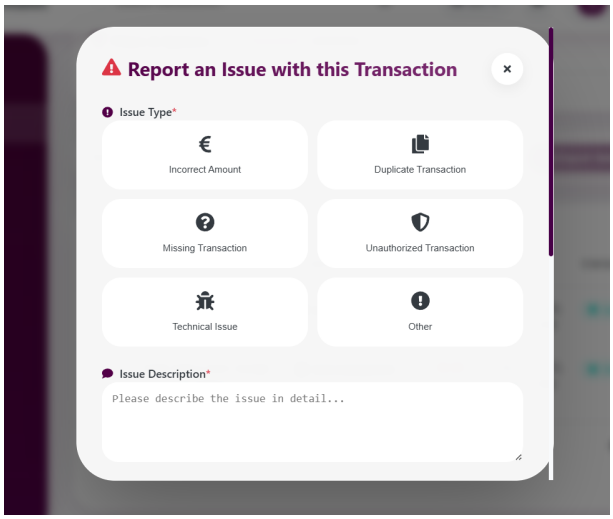


FIGURE 4.61 – Report issue of transactions

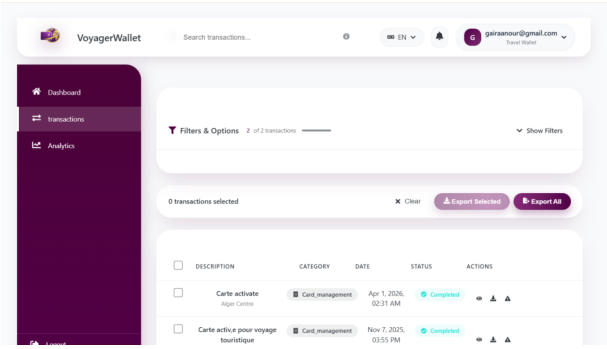


FIGURE 4.62 – Transaction management page

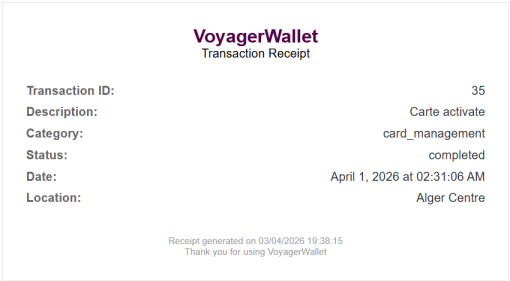


FIGURE 4.63 – Pdf file of transactions downloaded

4.7.5 Profile and account settings page

Profile and Account Settings page helps users manage security settings, for exemple change password and update personal informations. Also, users can see the connected devices to their account .

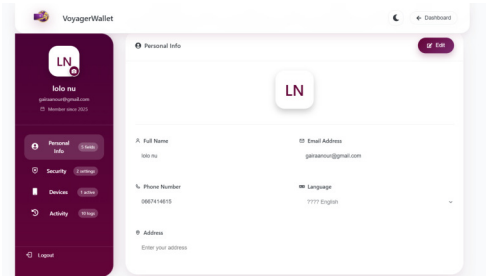


FIGURE 4.64 – Profile and account settings page(1)

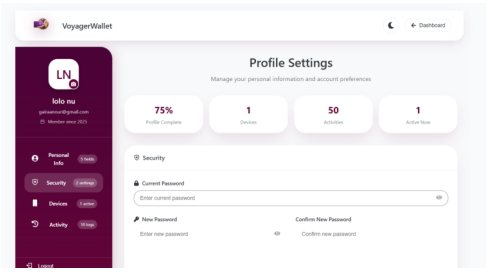


FIGURE 4.65 – Profile and account settings page(2)

4.7.6 Analytics page

This page gives you a look at how your tourism card is really being used. Here, you can easily see the status of your card : if it is active or not, if it has been suspended or if it has expired. You can also look at all the transactions that have been made using the card. You also have access to the Hourly Usage Pattern and the Daily Usage Pattern, giving you a better idea of how your card has been used. Under Card Lifecycle Events, you have the activation date and the expiration date. If there has been any blockage in using the card, you also have the Access Failure Reasons. This page is about openness and making it easy to manage your card.

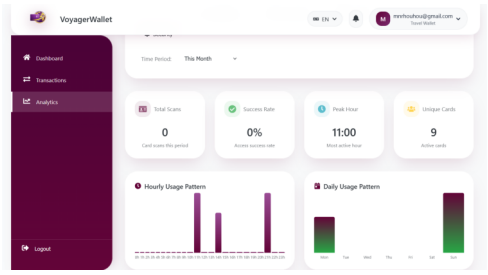


FIGURE 4.66 – Analytics page(1)

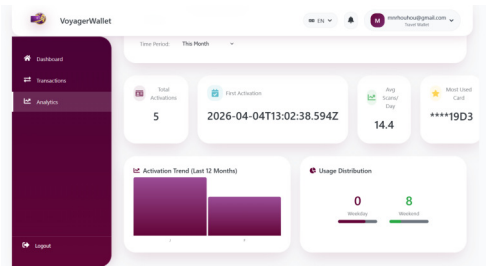


FIGURE 4.67 – Analytics page(2)

4.7.7 Administrator dashboard

The Administrator Dashboard is the main control interface of the Smart Card Validator application. It allows authorized administrators to monitor, control, and regulate all aspects of the Tourism Card system, such as users, card requests, cards issued, and analytics.

This Dashboard is developed with a secure authentication feature to ensure that only authorized personnel have access to sensitive financial and operational data. It provides administrators with monitoring capabilities, thereby facilitating uninterrupted management.

4.7.7.1 Admin dashboard(overview)

The Admin Dashboard is essentially the landing page, which provides a general overview of the entire system without going into detailed reports. This is a simple and clear overview of the system, which is exactly what is required of a landing page.

Here, we are displaying the total registered users and the total number of tourism cards issued. Furthermore, we are displaying the latest transactions , providing a real-time overview of the system.

The overview is essentially to provide a general idea of the system to the administrator, enabling them to understand the system and respond quickly.

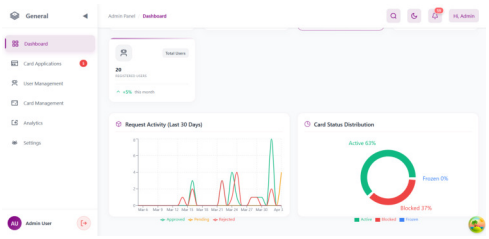


FIGURE 4.68 – Admin dashboard page(1)

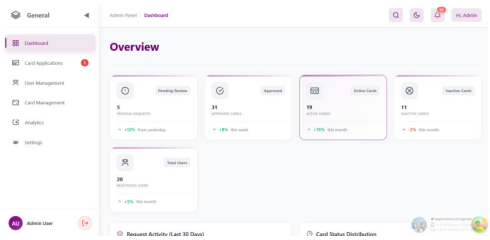


FIGURE 4.69 – Admin dashboard page(2)

4.7.8 User management page

The User Management page allows the administrator to manage all the registered users of the platform.

— View the list of registered users.
— Verify user identity before card approval.
— Track user activity.
— Search for users based on name, email, or date of registration.

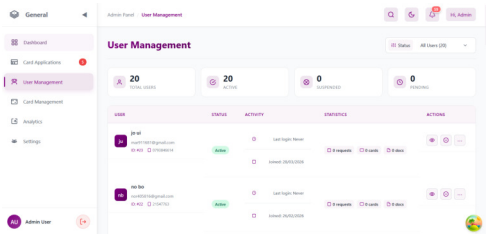


FIGURE 4.70 – User management page(1)

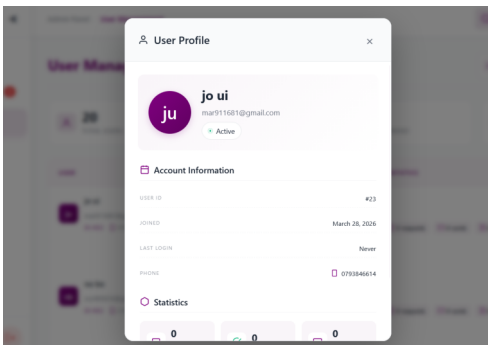


FIGURE 4.71 – User management page(2)

4.7.9 Card's request management page

The Card's Request Management interface allows administrators to manage all incoming requests to create the Tourism Card. Using the interface, administrators are able to :

— See all pending requests to create the card.
— Verify the documents provided by the user.
— Approve or deny the user's request to create the card.
— Track the status of the request, which can be either Pending, approved, or rejected.
— Send remarks for users that request for card if any missing documents for example.

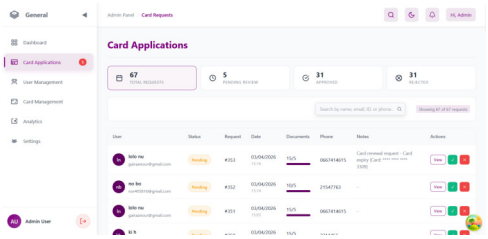


FIGURE 4.72 – Card's request management page(1)

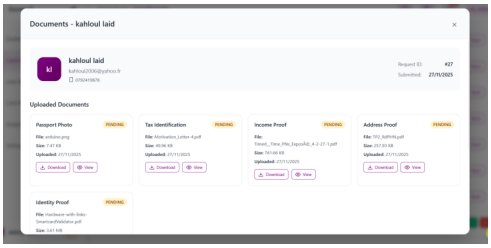


FIGURE 4.73 – Card's request management page(2)

4.7.10 Cards management page

The cards management page provides a comprehensive overview of all Tourism Cards. Specifically, it allows the administrator to :

— - View all active and inactive cards.
— - Monitor the balance and history of the cards.
— - block lost or suspicious cards.
— - Monitor statistics regarding the usage of the cards.

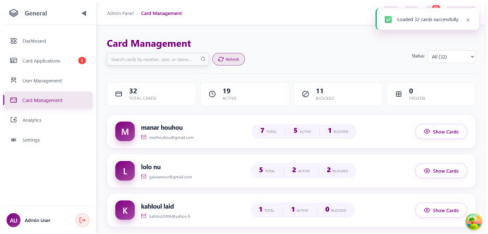


FIGURE 4.74 – Cards management page(1)

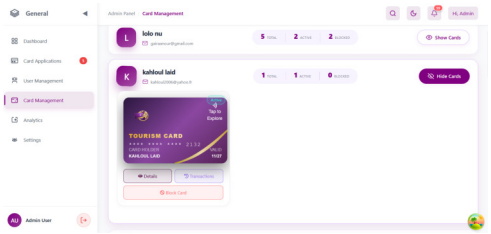


FIGURE 4.75 – Cards management page(2)

4.7.11 Analytics page

The Analytics Page provides statistical reports to help system administrators evaluate system performance and user behavior.

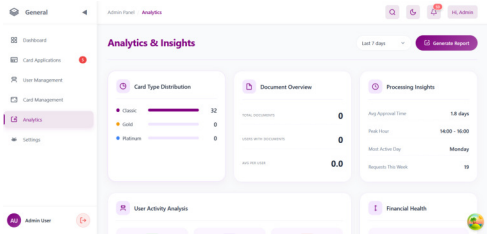


FIGURE 4.76 – Analytics page (1)

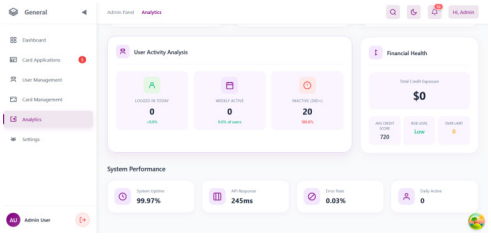


FIGURE 4.77 – Analytics page (2)

4.7.12 ATM network page

The ATM network admin Page provides admins with an overall view of the entire ATM network and an area specifically dedicated to finding and managing 'en panne' ATMs (out-of-order ATMs). The admin is provided with a real-time listing of all operational ATMs

as well as the out-of-order ones with information such as the location and time since the ATM was last online ,and error status — plus the ability to update each status.

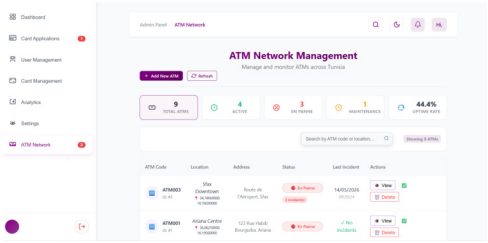


FIGURE 4.78 – ATM network page

4.7.13 Sub administrator dashboard

The system also includes a Sub-Administrator role with limited permissions compared to the main administrator. The Sub-Administrator can monitor ATM activities, view system information, and report technical or operational problems related to the SmartCard Validator devices.

When an issue is detected, such as device malfunction, connection failure, or transaction problems, the Sub-Administrator can send a problem report directly to the main administrator for further management and maintenance actions. This role helps improve system monitoring and ensures faster incident reporting without giving full administrative control.

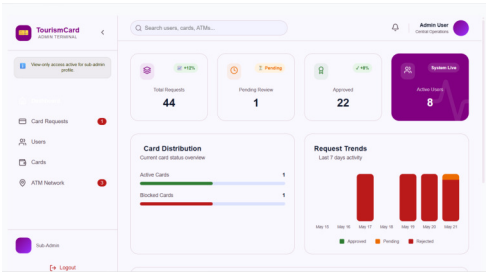


FIGURE 4.79 – Sub administrator dashboard(1)

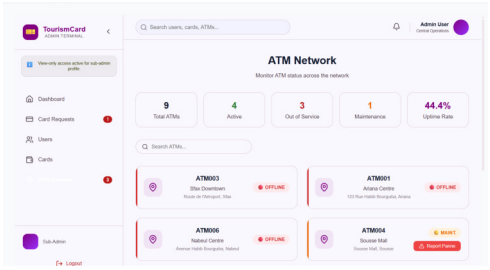


FIGURE 4.80 – Sub administrator dashboard(2)

4.8 Integration of GPS in the smartcard validator ATM

In our proposed system, a GPS module is integrated into the SmartCard Validator ATM device in order to determine the geographical location where the TourismCard activation takes place,when a traveler activates their card, the device reads its current GPS coordinates. These coordinates are transmitted securely to the backend server along with the card ID and timestamp.

The backend system compares the received coordinates with predefined authorized border locations. If the activation occurs within an approved border zone, the activation process is validated. Otherwise, the request is rejected,this mechanism ensures that TourismCard activation is restricted to official border points, improving transparency and security.

4.9 Security protocols

In the Smart Card validator system, security is paramount because of the sensitive nature of financial transactions and personal user data. The system incorporates various security protocols and mechanisms to provide confidentiality, integrity, authentication, and availability of information. This section describes the main security protocols used and justifies their importance.

4.9.1 Authentication and authorization

4.9.1.1 JWT based authentication

The system uses JSON Web Tokens (JWT) as a stateless authentication protocol. Upon successful login, a signed token containing the user ID, email, and role is generated using a 256-bit secret key. Tokens expire after 24 hours and are transmitted via the HTTP Authorization header. Each protected endpoint verifies the token before processing requests.

Why this choice JWT was selected because it enables stateless authentication, eliminating the need to store sessions on the server. This improves scalability and performance, especially in distributed systems. Additionally, JWT provides built-in integrity through cryptographic signatures.

4.9.1.2 Password security

User passwords are secured using the bcrypt hashing algorithm with 10 salt rounds. This method ensures resistance against rainbow table attacks through automatic salt generation. Passwords must meet the following criteria :

— Minimum length of 4 characters.
— At least 3 numeric digits.
— At least one special character.

Why this choice bcrypt was chosen because it is specifically designed for password hashing and is resistant to brute-force attacks due to its adaptive cost factor. The use of salting further enhances security by ensuring that identical passwords produce different hashes.

4.9.1.3 Authorization control

Access control is enforced using middleware :

— **authenticateToken** : Verifies JWT and attaches user data to requests.
— **authenticateAdmin** : Restricts access to administrative users.

Why this choice Middleware-based authorization allows centralized and reusable access control logic. This approach simplifies maintenance and ensures consistent enforcement of security policies across all endpoints.

4.9.2 Data protection

4.9.2.1 One way hashing

Sensitive data such as passwords and PINs are stored using bcrypt hashing. This ensures irreversible protection while allowing secure verification. Verification codes expire after 10 minutes.

Why this choice One-way hashing ensures that sensitive data cannot be recovered even if the database is compromised. This significantly reduces the risk of credential leakage and aligns with security best practices.

4.9.2.2 Two way encryption

PINs are additionally secured using AES-256-CBC encryption with a 256-bit key and random initialization vectors. This allows controlled decryption for administrative purposes.

Why this choice AES-256-CBC was selected due to its strong security and industry-wide adoption. It enables secure storage while still allowing controlled access when decryption is required for administrative operations.

4.9.2.3 Dual PIN storage

The database maintains two representations of PINs :
— `pin_hash` : bcrypt hash for authentication.
— `pin_encrypted` : AES-256-CBC encrypted value for administrative access.

Why this choice This dual approach balances security and functionality. Hashing ensures secure user authentication, while encryption allows administrative retrieval when necessary without compromising overall system security.

4.9.3 Transport layer security

4.9.3.1 HTTPS communication

All client-server and external communications use HTTPS with TLS 1.2 or higher, ensuring data confidentiality and integrity.

Why this choice HTTPS with TLS protects data in transit against eavesdropping and man-in-the-middle attacks. It is a standard requirement for secure web applications and ensures user trust.

4.9.3.2 Email security (STARTTLS)

Emails are transmitted using SMTP with STARTTLS encryption via Gmail servers (port 587), ensuring secure delivery of sensitive information.

Why this choice STARTTLS upgrades plain SMTP connections to encrypted ones, providing confidentiality without requiring a separate secure port. This makes it widely compatible and easy to deploy.

4.9.4 External communication

4.9.4.1 HTTPS APIs

The system integrates external services using HTTPS :
— OpenWeatherMap for weather data.
— OpenStreetMap Nominatim for geolocation.
— ipapi.co for IP-based location fallback.

Why this choice Using HTTPS ensures that all third-party communications are encrypted and secure. It also guarantees data integrity and authenticity of responses from external services.

4.9.4.2 WhatsApp business API

Notifications are sent via the WhatsApp Business API over HTTPS with end-to-end encryption. Use cases include :
— Card approval notifications.
— PIN delivery.
— Security alerts.

Why this choice WhatsApp API was chosen due to its high delivery rate and user engagement. End-to-end encryption ensures message confidentiality, making it a secure alternative to traditional SMS.

4.9.5 Database communication

4.9.5.1 PostgreSQL protocol

Communication with the PostgreSQL database uses the native wire protocol over SSL-encrypted connections.

Why this choice The PostgreSQL protocol provides efficient and reliable database communication. SSL encryption ensures that sensitive data exchanged with the database is protected.

4.9.5.2 Secure query handling

Parameterized queries ($1, $2) are used to prevent SQL injection attacks.

Why this choice Parameterized queries separate SQL logic from user input, effectively eliminating SQL injection vulnerabilities, which are among the most common web security threats.

4.9.5.3 Connection pooling

A connection pool (pg Pool) maintains multiple active connections, improving performance and reducing latency.

Why this choice Connection pooling reduces the overhead of repeatedly opening and closing database connections, leading to better performance and scalability.

4.9.5.4 Transaction management

ACID-compliant transactions ensure atomic and consistent database operations.

Why this choice Transactions guarantee data consistency and reliability, especially for critical operations such as financial or account-related updates.

4.9.6 Email communication

4.9.6.1 SMTP with TLS

The system uses SMTP with TLS for sending :
— Verification emails.
— Password reset links.
— Notifications and alerts.

Why this choice SMTP with TLS ensures secure and standardized email delivery. It is widely supported and suitable for transmitting sensitive user notifications.

4.9.6.2 Reliability

The implementation includes retry mechanisms and delivery tracking to ensure message delivery.

Why this choice Reliable delivery mechanisms are critical for security-related communications such as password resets and alerts, ensuring users receive important information without failure.

4.9.7 File upload security

4.9.7.1 Multipart data handling

File uploads use multipart/form-data encoding, allowing transmission of files and metadata in a single request.

Why this choice Multipart encoding is the standard method for file uploads in web applications, enabling efficient and structured data transmission.

4.9.7.2 Validation

Strict validation rules are applied :
— Allowed formats : JPEG, PNG, PDF.
— Maximum size : 5MB.
— MIME type verification.

Why this choice Strict validation prevents malicious file uploads and reduces risks such as code execution or storage abuse.

4.9.7.3 Secure storage

Files are stored outside the public web directory and accessed only through authenticated requests.

Why this choice Storing files outside the public directory prevents direct access via URL, ensuring that only authorized users can retrieve sensitive documents.

4.9.8 AI based fraud detection

4.9.8.1 Detection agent

The system integrates an intelligent fraud detection agent that monitors user activities and transactions in real time.

The agent is based on a set of behavioral rules designed to detect suspicious activities, including :
— Multiple failed PIN attempts (3 wrong attempts within 1 minute).
— Simultaneous transactions from different countries.
— Unusual transaction amount compared to normal user behavior.
— Rapid successive transactions in a short time interval.
— Transactions from a new or unknown device.
— Inconsistent IP address or sudden geographic change.

Why this choice These rules reflect common fraud patterns observed in real financial systems. For example, repeated failed authentication attempts indicate brute-force attacks, while geographically inconsistent transactions suggest card cloning. Behavioral anomalies such as unusual amounts or new devices may indicate unauthorized access.

4.9.8.2 System reaction

When suspicious behavior is detected :
— The transaction is flagged or rejected.
— The card may be temporarily blocked (in high-risk cases).
— The event is logged in the system.
— The administrator is notified for verification.

Why this choice This layered response ensures both security and flexibility. Critical threats trigger immediate blocking, while less severe anomalies are flagged for human review, reducing false positives.

4.9.8.3 Limitations

This approach is rule-based and does not rely on machine learning. It detects predefined fraud scenarios but may not identify complex or previously unseen attack patterns.

Why this choice A rule-based system is simple to implement, fast in execution, and effective for detecting well-known fraud behaviors. It also provides a solid foundation for future integration of advanced AI or machine learning models.

4.10 Product prototype

The proposed prototype is a smart tourism allowance management system based mainly on the Smart Tourism Card and the SmartCard Validator Device. The validator device, installed at airports and border points, securely activates the tourism card before departure after verifying the traveler's information. Once activated, the card can be used abroad to access the tourism allowance securely. To complete the traveler usage scenario, we also added a purchase/payment device that allows travelers to use the activated card for international payments and purchases.



FIGURE 4.81 – Picture of our activation ATM



FIGURE 4.82 – Picture of our tourism card



FIGURE 4.83 – Picture of our purshace device

4.11 System maintenance strategy

To ensure the long-term reliability, security, availability, and operational efficiency of the SmartCard Validator System after deployment, a complete maintenance strategy has been proposed. Since the system is intended to manage sensitive financial operations and tourism card activations at border locations, maintaining the device properly is essential to avoid service interruption, security vulnerabilities, and hardware failures.

The maintenance strategy combines preventive maintenance, corrective maintenance, predictive maintenance, software maintenance, hardware inspection, remote monitoring, troubleshooting, firmware updating, and cybersecurity management.

4.11.1 Objectives of maintenance

The main objectives of the maintenance process are :
— Ensure continuous operation of the SmartCard Validator Device.
— Prevent unexpected hardware and software failures.
— Detect abnormal behavior and security threats.
— Improve device reliability and operational stability.
— Reduce system downtime and maintenance costs.
— Ensure secure and stable communication with the backend server.

4.11.2 Maintenance categories

The proposed maintenance strategy is divided into four major categories.

4.11.2.1 Preventive maintenance

Preventive maintenance refers to periodic maintenance operations performed before failures of the device occur.

Examples of preventive maintenance include :

— Periodic testing of the NFC reader.
— Verification of LCD screen functionality.
— Inspection of keypad buttons.
— Cleaning internal hardware components.
— Monitoring Wi-Fi signal stability.
— Checking power supply voltage stability.
— Updating firmware and security patches.

Preventive maintenance minimizes operational interruption and improves overall system reliability.

4.11.2.2 Corrective maintenance

Corrective maintenance is performed after detecting a hardware or software failure. Its purpose is to restore the system to normal operation.

Examples include :

— Replacing damaged NFC modules.
— Repairing keypad failures.
— Resolving Wi-Fi connectivity problems.
— Fixing backend communication errors.
— Replacing defective power components.
— Correcting software bugs detected during operation.

Corrective maintenance ensures rapid recovery after failures.

4.11.2.3 Predictive maintenance

Predictive maintenance uses monitoring mechanisms to identify abnormal conditions before critical failure occurs.

The system may monitor :

— CPU temperature of the ESP32.
— Frequency of unexpected reboots.
— Internet connection stability.
— Power consumption anomalies.
— GPS signal quality.
— Repeated hardware communication failures.

This maintenance approach helps administrators intervene before complete device failure occurs.

4.11.2.4 Security maintenance

Security maintenance protects the system against evolving cybersecurity threats.

Security maintenance operations include :

— Firmware security patch updates.
— API key rotation.
— Password and credential management.
— Monitoring suspicious login attempts.

— Detecting abnormal transaction patterns.
— Updating authentication mechanisms.
— Reviewing access permissions and user roles.

Because the system handles financial operations, cybersecurity maintenance is considered a continuous process.

4.11.3 Hardware maintenance

The SmartCard Validator Device integrates several hardware components that require periodic inspection and testing.

4.11.3.1 ESP32 microcontroller maintenance

The ESP32 acts as the central processing and communication unit of the device.

Maintenance operations include :

— Monitoring overheating issues.
— Detecting unexpected restarts.
— Verifying firmware stability.
— Checking memory usage.
— Ensuring stable communication with peripherals.

4.11.3.2 NFC Reader maintenance

The NFC reader is responsible for reading Tourism Cards and validating user interaction.

Maintenance tasks include :

— Testing card detection accuracy.
— Verifying communication stability with the ESP32.
— Cleaning the reader surface.
— Detecting read timeout errors.

4.11.3.3 LCD screen maintenance

The LCD display provides instructions and feedback to users.

Maintenance includes :

— Checking display readability.
— Detecting dead pixels or communication errors.

4.11.3.4 Keypad maintenance

The keypad is used for PIN entry and user interaction.

Maintenance tasks include :

— Testing all keypad buttons.
— Detecting delayed or failed inputs.
— Replacing damaged keys if necessary.

4.11.3.5 GPS Module maintenance

The GPS module verifies activation location.

Maintenance operations include :

— Verifying GPS signal reception.
— Checking coordinate accuracy.
— Detecting satellite synchronization issues.

4.11.3.6 Wi-Fi connectivity maintenance

The Wi-Fi module ensures backend communication.
Maintenance includes :
— Verifying internet connectivity.
— Detecting communication interruptions.
— Testing reconnection mechanisms.

4.11.3.7 Power supply maintenance

Stable power is critical for system reliability.
Maintenance operations include :
— Monitoring voltage stability.
— Inspecting power adapters and cables.
— Verifying backup battery systems.

4.11.4 Software maintenance

Software maintenance ensures proper system functionality and security.

4.11.4.1 Firmware updates

Firmware updates improve device functionality and security.
The update process may include :
— Bug fixing.
— Performance optimization.
— Security patching.
— Addition of new features.

4.11.4.2 Backend maintenance

The backend server also requires continuous maintenance.
Maintenance operations include :
— API optimization.
— Database indexing and optimization.
— Log monitoring.
— Error correction.
— Security patch management.
— Performance monitoring.

4.11.5 Self diagnostic system

To improve reliability, the SmartCard Validator Device can implement a self-diagnostic mechanism executed during startup.
The self-diagnostic procedure verifies :
— Wi-Fi connectivity.

— NFC reader functionality.
— GPS module availability.
— LCD communication.
— Backend API accessibility.
— Memory availability.
— Power system status.

If an error is detected, the system displays an error message on the LCD screen and stores the error in the device log.

Examples of possible error codes include :

— WIFI_ERROR.
— NFC_TIMEOUT.
— GPS_NOT_FOUND.
— API_FAILED.
— POWER_INSTABILITY.

4.11.6 Remote monitoring system

The backend platform can monitor deployed devices remotely in real time.

The monitoring dashboard may display :

— Device online/offline status.
— Device GPS location.
— Last synchronization timestamp.
— Firmware version.
— Number of failed activation attempts.
— System error logs.
— Device health indicators.

This mechanism allows administrators to detect failures rapidly and improve operational efficiency.

4.11.7 Database backup and recovery

Since the backend database stores critical financial information, periodic backups are necessary.

Backup strategies include :

— Daily database backup.
— Transaction log storage.
— Cloud backup replication.
— Disaster recovery procedures.

These mechanisms ensure data integrity and rapid restoration after failure.

4.12 Conclusion

This chapter detailed the implementation and realization process of the proposed **SmartCard Validator System**. The web application was developed using React, while the mobile application was implemented using React Native. The hardware prototype was programmed in C++ using the ESP32 microcontroller and integrated with several electronic components including the RFID/NFC reader, keypad, LCD display, buzzer, battery, and GPS module.

The implemented system successfully performs the main operations related to the activation and management of the tourism allowance smart card, transaction monitoring, user interaction, and location tracking. In addition, several security mechanisms were integrated to ensure data protection, secure communication, authentication, and fraud detection.

The developed interfaces provide an easy and user-friendly experience for travelers, administrators, and banking services, while the hardware prototype demonstrates the feasibility of deploying the system at airports and border points. Overall, the implementation confirms the practicality, scalability, and effectiveness of the proposed solution in modernizing the management of the tourism allowance in algeria.

Chapitre 5

Conclusion and Perspectives

5.1 Conclusion

Banks face difficulties in managing currency exchange, especially at airports and border areas, due to heightened demand, long queues, limited foreign currency access, and slow manual procedures. At the same time, travelers face hurdles such as delays, difficulties in acquiring foreign currency, and a lack of smooth and reliable financial services.

This initiative proposes a smart digital approach to tackle these challenges, employing a prepaid card system, a validation tool, an online platform, and a mobile application. This unified system simplifies banking procedures and improves the experience for travelers.

It facilitates rapid, secure, and cashless payments, reduces dependence on traditional banking practices, and enhances control and efficiency in currency exchange processes.

Prepaid tourism smart cards have been introduced from the onset, and the limitations of cash and card transactions have been analyzed. The project's foundational technologies include near-field communication and chip card interfaces, authentication, encryption, network communication, and the integration of web and mobile technologies, with a major emphasis on transactional security.

Architectural models and diagrams have been used to represent the analysis and design of the system, showing how the smart card, the validation device, the server, the website, and the mobile app interact with each other. This formed the foundation for a system that is both safe, reliable, and consistent in its workflow.

In the implementation of the project, the embedded system in the device, the development technologies for the website and mobile apps, and the security of the system, including the encryption of data and its interaction, have been addressed. In fact, the approach proved to be both effective and safe for the activation, validation, and management of the card via the website and mobile app, despite the challenges encountered in terms of hardware compatibility and communication.

5.2 Perspectives

However, several aspects of this study might be improved, which we see as promising for our work.

— Secure offline functionality ensures that the system remains operational in areas with poor or no internet connectivity.

— Improving system security by implementing stronger cryptographic protocols, and more robust fraud detection mechanisms.
— Extending the system to support multi-currency and multi-country usage, allowing tourists to use the same card across different destinations while complying with local regulations.
— Enhancing device hardware by reducing power consumption, improving durability, and integrating newer communication technologies for faster and more reliable transactions.
— The system enhances user authentication by integrating biometric fingerprint technology, and supports EMV chip card technology.
— Our project will be developed to integrate multiple card types, including a business manager card and a student card, to go beyond tourism only.

References

[1] Tertag Wissam Mezhoudi Ahlem. A wearable smart device to track and find the alzheimer's patient's location.

[2] Bala Krishna AV et al. Hdfc bank-a fab 50 company. *IPE Journal of Management*, 7(1), 2017.

[3] Marek Babiuch, Petr Foltỳnek, and Pavel Smutnỳ. Using the esp32 microcontroller for data processing. In *2019 20th International Carpathian Control Conference (ICCC)*, pages 1–6. IEEE, 2019.

[4] HDFC Bank. Multicurrency platinum forexplus chip forex card. https://www.hdfc.bank.in/forex-cards/multicurrency-platinum-forexplus-chip-forex-card, 2026. Accessed February6,2026. Information about features, benefits, and travel usage.

[5] Standard Chartered Bank. Travel card – standard chartered bangladesh. https://www.sc.com/bd/deposits/travel-card/, 2026. Accessed February 6, 2026. Information on features, travel quota, and card usage.

[6] Bhavik Bhatt and Muskaan Nandu. An overview of structural uml diagrams. *International Research Journal of Engineering and Technology*, 8(8) :1577–1583, 2021.

[7] Bohdan Borowik. Matrix keypad+ serial transmission. In *Interfacing PIC Microcontrollers to Peripherial Devices*, pages 105–127. Springer, 2011.

[8] Greg Boss, Padma Malladi, Dennis Quan, Linda Legregni, and Harold Hall. Cloud computing. *IBM white paper*, 321 :224–231, 2007.

[9] Jeffrey F Bull. Wireless geolocation. *IEEE Vehicular Technology Magazine*, 4(4) :45–53, 2009.

[10] Nimesh Chhetri. A comparative analysis of node. js (server-side javascript). 2016.

[11] U. Chirico. *Smart Card Programming*. Lulu.com, 2014.

[12] Wikipedia contributors. Iso c++ logo. https://gpsuite.fr/en/content/9-what-is-gps, 2025. Accessed November 6, 2025.

[13] Wikipedia contributors. Iso c++ logo. https://medium.com/navixy/alternatives-to-gps-location-tracking-with-gsm-and-wifi-2a94f837296a, 2025. Accessed November 6, 2025.

[14] Wikipedia contributors. Iso c++ logo. https://www.fundz.net/blog/how-accurate-is-ip-geolocation-a-guide-for-businesses-and-security-pros, 2025. Accessed November 6, 2025.

[15] Wikipedia contributors. Iso c++ logo. https://commons.wikimedia.org/wiki/File:C_Programming_Language.svg, 2025. Accessed November 6, 2025.

[16] Vedat Coskun, Kerem Ok, and Busra Ozdenizci. *Professional NFC application development for android*. John Wiley & Sons, 2013.

[17] Ryan Dahl. Node.js logo. https://upload.wikimedia.org/wikipedia/commons/d/d9/Node.js_logo.svg, 2016. Licensed under the Expat (MIT) License. Accessed November 6, 2025.

[18] François De Keersmaeker, Nicolas van de Walle, Yves Deville, and Ramin Sadre. Using lorawan and wi-fi for smart city monitoring in louvain-la-neuve.

[19] Icon-Icons / Devicon. React original wordmark logo. https://icon-icons.com/icon/react-original-wordmark-logo/146375, 2020. Free for commercial use according to the source. Accessed November 6, 2025.

[20] Icon-Icons / Devicon. React original wordmark logo. https://pgadmin-4.macupdate.com/app/mac/60968/pgadmin-4/old-versions, 2020. Free for commercial use according to the source. Accessed November 6, 2025.

[21] Icon-Icons / Devicon. React original wordmark logo. https://commons.wikimedia.org/wiki/File:Arduino_IDE_logo.svg, 2020. Free for commercial use according to the source. Accessed November 6, 2025.

[22] Icon-Icons / Devicon. React original wordmark logo. https://arduino-projekte.info/products/d1-mini-esp32-wifi-bluetooth?srsltid=AfmBOopWIBN28hmNoLjxkRZtZpnfOHuf__FEzbUxLpPvP20h7oOQhQed, 2020. Free for commercial use according to the source. Accessed November 6, 2025.

[23] Tomás Domínguez-Bolaño, Omar Campos, Valentín Barral, Carlos J Escudero, and José A García-Naya. An overview of iot architectures, technologies, and existing open-source projects. *Internet of Things*, 20 :100626, 2022.

[24] John Fallows. Nfc tags — how they work, 2017.

[25] Mohamed Fezari and Ali Al Dahoud. Integrated development environment "ide" for arduino. *WSN applications*, 11 :1–12, 2018.

[26] Cory Gackenheimer. *Introduction to React*. Apress, 2015.

[27] Alexandros Gazis. What is iot ? the internet of things explained. *Academia Letters*, 2, 2021.

[28] X Gong, F Erwee, and Victoria Rautenbach. Geometry viewer for pgadmin4 : A process guided by the google summer of code. International Society for Photogrammetry and Remote Sensing, 2019.

[29] Caiyong Hao, Daquan Feng, Qinyu Zhang, and Xiang-Gen Xia. Interference geolocation in satellite communications systems : An overview. *IEEE Vehicular Technology Magazine*, 16(1) :66–74, 2020.

[30] Havizul Havizul et al. Design of a relay circuit based lcc bell for the iain pontianak quiz competition. *Circuit : Jurnal Ilmiah Pendidikan Teknik Elektro*, 7(2) :106–116, 2023.

[31] Zi Hu, John Heidemann, and Yuri Pradkin. Towards geolocation of millions of ip addresses. In *Proceedings of the 2012 Internet Measurement Conference*, pages 123–130, 2012.

[32] Nishtha Jatana, Sahil Puri, Mehak Ahuja, Ishita Kathuria, and Dishant Gosain. A survey and comparison of relational and non-relational database. *International Journal of Engineering Research & Technology*, 1(6) :1–5, 2012.

[33] Beauden John. A comparative analysis of the significance of use case and sequence diagrams focus on small-scale projects. 2025.

[34] Md Dalawar Kawsar. *Credit Card of Standard Chartered Bank*. PhD thesis, East West University, 2008.

[35] Nallapaneni Manoj Kumar and Pradeep Kumar Mallick. The internet of things : Insights into the building blocks, component interactions, and architecture layers. *Procedia computer science*, 132 :109–117, 2018.

[36] Chunyan Li. Working with liquid crystal display. In *Record Weather Data with Arduino and Solar Power : Use Sensors to Record and Analyze Meteorological Data*, pages 81–103. Springer, 2024.

[37] Soumik Mandal and Arko Biswas. Cloning of radio frequency identification (rfid) card using rc-522 module.

[38] Sheli McHugh and Kristen Yarmey. What is nfc ? *Near Field Communication : Recent Developments and Library Implications*, pages 5–13, 2022.

[39] Md Rifat Mondol. *Design and Implementation of Radio Frequency Identification (RFID), Keypad & GSM based Security Access Control*. PhD thesis, DAFFODIL INTERNATIONAL UNIVERSITY, 2023.

[40] SS Mule, Y Waykar, and Swami Vivekanand Mahavidyalaya. Role of use case diagram in s/w development. *International Journal of Management and Economics*, 2015.

[41] React Native. React native. *Acesso em*, 30, 2024.

[42] SPES Nawarathna. *Automation of Currency Exchange Process at the Bank of Ceylon Pay Office*. PhD thesis, 2024.

[43] Oksana Nikiforova, Janis Sejans, and Antons Cernickins. Role of uml class diagram in object-oriented software development. *Sci. J. Riga Tech. Univ. Ser. Comput. Sci.*, 44 :65–74, 2011.

[44] Masayuki Okuhara, Tetsuo Shiozaki, and Takuya Suzuki. Security architecture for cloud computing. *Fujitsu Sci. Tech. J*, 46(4) :397–402, 2010.

[45] Jennifer Robbins. *Learning Web Design : A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics*. O'Reilly Media, Inc., 2012.

[46] Rudloff. Css3 logo and wordmark. https://commons.wikimedia.org/wiki/File:CSS3_logo_and_wordmark.svg, 2016. Licensed under the Creative Commons Attribution 3.0 Unported License. Accessed November 6, 2025.

[47] Hukum Saini, Abhay Upadhyaya, and Manish Kumar Khandelwal. Benefits of cloud computing for business enterprises : A review. In *Proceedings of International Conference on Advancements in Computing & Management (ICACM)*, 2019.

[48] Anna Sainsbury. Geolocation basics. *Gaming Law Review and Economics*, 17(1) :33–35, 2013.

[49] Stack Code Training. React native course, 2026. Accessed : 2026-04-04.

[50] Veda C Storey. Relational database design based on the entity-relationship model. *Data & knowledge engineering*, 7(1) :47–83, 1991.

[51] Bjarne Stroustrup. An overview of c++. In *Proceedings of the 1986 SIGPLAN workshop on Object-oriented programming*, pages 7–18, 1986.

[52] Travelex. Travelex money card – travel money card. https://www.travelex.com.au/travel-money-card, 2026. Accessed February 6, 2026. Information about the Travelex Money Card features, currencies, and benefits.

[53] Guochang Xu. *GPS : theory, algorithms and applications*. Springer, 2007.

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد خيضر- بسكرة-

عنوان المشروع:

نظام التفعيل الذكي لبطاقة منحة السياحة

مشروع لنيل شهادة مؤسسة ناشئة في اطار القرار الوزاري 1275

صورة العلامة التجارية

الاسم التجاري

Tourism Card

السنة الجامعية :

2026/2025

بطاقة معلومات:

حول فريق الاشراف وفريق العمل

1-فريق الاشراف:

فريق الاشراف	
المشرف الرئيسي: كحلول العيد	التخصص: إعلام الآلي
المشرف المساعد(01): محمدرمضاني	التخصص: إعلام الآلي
المشرف المساعد(02): محمد جلاب	التخصص: العلوم الاقتصادية

2-فريق العمل:

فريق المشروع	التخصص	الكلية
الطالبة: قرع نور الهدى	هندسة البرمجيات والأنظمة الموزعة	العلوم الدقيقة
الطالبة: مزوري سيرين	هندسة البرمجيات والأنظمة الموزعة	العلوم الدقيقة
الطالبة: حوحو منار	نظام المعلومات وتحسين اتخاذ القرار	العلوم الدقيقة

فهرس المحتويات

المحور الأول: تقديم المشروع

المحور الثاني: الجوانب الابتكارية

المحور الثالث: التحليل الاستراتيجي للسوق

المحور الرابع: خطة الإنتاج والتنظيم

المحور الخامس :الخطة المالية

المحور السادس : النموذج الاولي التجريبي

المحور الأول: تقديم المشروع

1. تعريف عام بالمشروع (الوضع المقترح)

تعاني عملية صرف المنحة السياحية المقدرة بـ 750 يورو في الجزائر من عدة مشاكل مرتبطة بالإجراءات التقليدية المعتمدة حاليًا، حيث تشهد البنوك ضغطًا كبيرًا أثناء عمليات التحقق وصرف العملة، إضافة إلى طول مدة الانتظار، تعقيد الإجراءات الإدارية، وصعوبة تتبع العمليات المالية بشكل دقيق وآمن. كما تواجه المؤسسات البنكية تحديات لوجستية وأمنية مرتبطة بنقل وتوزيع العملة الأجنبية عبر مختلف نقاط العبور.

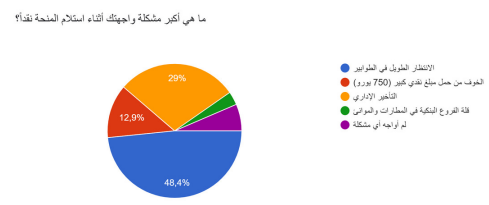
ومع التطور المتسارع في مجال الرقمنة واعتماد الأنظمة الذكية في القطاعين المالي والسياحي، أصبح من الضروري توفير حل حديث يساهم في تحسين جودة الخدمات وتسهيل تجربة المسافرين بطريقة أكثر أمانًا وفعالية.

في هذا الإطار، يهدف مشروعنا إلى تطوير نظام ذكي لرقمنة وتسيير المنحة السياحية من خلال بطاقة سياحية إلكترونية مرتبطة بجهاز تحقق ذكي يسمى *SmartCard Validator* ، إضافة إلى منصة ويب وتطبيق هاتفي يسمحان بإدارة البطاقات، متابعة العمليات، وتحسين مراقبة النظام بشكل لحظي وآمن.

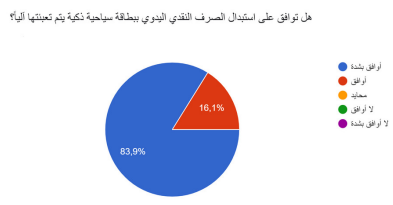
ويقدم المشروع مجموعة من الحلول أهمها:

- ❑ تقليل الضغط على البنوك أثناء عمليات صرف المنحة السياحية بنسبة قد تصل إلى 70%.
- ❑ تسريع إجراءات التحقق وتفعيل البطاقة من عدة ساعات قد تتجاوز 4 أو 5 ساعات إلى بضع دقائق فقط.
- ❑ تحسين تتبع العمليات المالية ومراقبتها بشكل لحظي مع تقليل أخطاء المعالجة بنسبة كبيرة.
- ❑ توفير خدمات رقمية آمنة وسهلة للمسافرين مع تحسين تجربة المستخدم وتقليل مدة الانتظار بأكثر من 80%.
- ❑ تقليل الاعتماد على التعاملات النقدية التقليدية وتقليص مخاطر نقل الأموال الأجنبية عبر نقاط العبور.

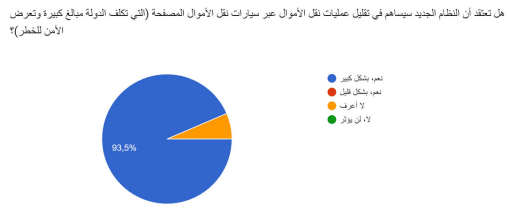
استبيان إحصائي لدراسة جدوى المشروع



شكل 1: Stat 1



شكل 2: Stat 2



شكل 3: Stat 3

2. القيمة المضافة للمشروع

يقدم هذا المشروع قيمة مضافة كبيرة، خاصة للبنوك، من خلال:

- ✔ تقليل الضغط على فروع البنوك بنسبة تصل إلى **70%** وتقليص عدد المعاملات اليدوية.
- ✔ تسريع عملية التحقق وتحويل العملات من **4-5 ساعات** إلى أقل من **5 دقائق**.
- ✔ خفض التكاليف التشغيلية للبنوك بنسبة تقارب **40%** بفضل أتمتة العمليات وتقليل الحاجة إلى الموارد البشرية.
- ✔ تعزيز الأمان من خلال استخدام تقنيات التشفير والتحقق الذكي من البطاقات مع تقليل مخاطر الأخطاء بنسبة **60%**.
- ✔ تحسين تتبع العمليات وضمان الشفافية من خلال تسجيل **100%** من العمليات بشكل رقمي وفوري.
- ✔ تقديم حل مبتكر يعتمد على البطاقات الذكية وتقنيات NFC لتحديث الخدمات البنكية الرقمية.

كما يوفر للمسافر:

- ✔ الحصول على المنحة السياحية بطريقة سريعة وسهلة مع تقليص وقت الخدمة من ساعات إلى دقائق.
- ✔ تقليص فترات الانتظار داخل الوكالات البنكية بنسبة تصل إلى **80%**.
- ✔ الاستفادة من بطاقة ذكية واحدة لتنفيذ مختلف العمليات المرتبطة بالمنحة.
- ✔ خدمة متاحة بسرعة أكبر وبتكلفة أقل مقارنة بالمعالجة التقليدية.
- ✔ تجربة استخدام حديثة تعتمد على التكنولوجيا الرقمية والابتكار.

3. فريق العمل

الطالبة	المهام	التكوين
حوحو منار	تطوير التطبيق، تطوير الواجهة الخلفية للمنصة (Backend)، وإنجاز النموذج الأولي للجهاز	لديها دورة تكوينية في تسويق المنتجات والخدمات، ودورة في التقطيع بالليزر، إضافة إلى تدريب في SolidWorks، كما تلقت أساسيات في Arduino وتطوير واجهات المستخدم (UI/UX) وأساسيات البرمجة، إضافة إلى تربص ميداني في مؤسسة اتصالات الجزائر.
قيرع نور الهدى	تصميم وبرمجة المنصة (Backend,Fronend)، ودعم تطوير الجهاز	لديها دورة تكوينية في تسويق المنتجات والخدمات، ودورة في التقطيع بالليزر، إضافة إلى تدريب في SolidWorks، كما درست تصميم واجهات المستخدم، وقواعد البيانات، وأساسيات الشبكات، إضافة إلى تربص ميداني في مؤسسة اتصالات الجزائر.
مزوري سيرين	تصميم وبرمجة المنصة (Backend,Fronend)، ودعم تطوير الجهاز	لديها دورة تكوينية في تسويق المنتجات والخدمات، ودورة في التقطيع بالليزر، إضافة إلى تدريب في SolidWorks، كما تلقت تكوينًا في إدارة المشاريع، وتحليل النظم، وأساسيات الأمن المعلوماتي، إضافة إلى تربص ميداني في كل من مؤسسة اتصالات الجزائر ومؤسسة بريد الجزائر.

4. أهداف المشروع

يهدف هذا المشروع إلى تقديم حل عملي يساهم في تطوير الخدمات السياحية من خلال اعتماد نظام ذكي للتحقق من البطاقة السياحية.

ومن خلال هذا المشروع نسعى إلى تحقيق ما يلي:

- المساهمة في رقمنة الخدمات السياحية عبر نظام ذكي مرتبط بالنظام البنكي.
- توفير نظام آمن يقلل من مخاطر التزوير.
- تصميم جهاز لتفعيل البطاقة السياحية قبل السفر.
- إنشاء منصة إلكترونية وتطبيق لإدارة المعاملات.
- تحسين تجربة المستخدمين.
- توفير واجهات سهلة الاستخدام.

5. الجدول الزمني لتحقيق المشروع

الأعمال	1	2	3	4	5	6
الدراسات الأولية	✓	✓	✓			
طلب المعدات		✓	✓			
تركيب المعدات				✓	✓	
تطوير النموذج الأولي						✓
البرمجة والتطوير	✓	✓	✓	✓	✓	

المحور الثاني: الجوانب الابتكارية

1. طبيعة الابتكار

ينعكس الابتكار في مشروعنا من خلال إنشاء نظام ذكي ومتكامل للتحقق من بطاقات السياحة. يتم بناء هذا النظام على بطاقة سياحية إلكترونية متصلة بجهاز تحقق ذكي ومنصة رقمية شاملة من أجل رقمنة المنحة السياحية المقدرة ب 750 اورو من خلال بطاقة واحدة مع محتوى محدد من أجل منح السائح فرصة الوصول للخدمات عبر وسيلة واحدة بسرعة وفعالية.

ينطوي مشروعنا على دمج العديد من التقنيات الحديثة من أجل تحقيق الابتكار، مثل الاتصال قريب المدى ،(NFC) وتحديد الموقع الجغرافي ،(GPS) وتكنولوجيا تشفير البيانات، مما يتيح تحقق بطاقة السياحة بشكل فوري من حيث صلاحيته ومحتواها من أجل الاستخدام في الوقت الحقيقي من خلال منصة إلكترونية وتطبيق مخصص.

2. مجالات الابتكار

تماشيًا مع ذلك، يُظهر مشروع نظام التحقق الذكي للبطاقة السياحية وجود العديد من مجالات الابتكار، والتي تتمثل فيما يلي:

الابتكار التكنولوجي: تصميم جهاز تحقق ذكي مدمج يُعرف باسم *Smart Card Validator* يحتوي على قارئ بطاقات بتقنية ،NFC إضافة إلى نظام تحديد الموقع الجغرافي ،(GPS) مع اعتماد آليات تشفير لبيانات التحقق لضمان الأمان وصحة العمليات.

الابتكار الرقمي: إنشاء منصة ويب وتطبيق جوال يتيحان إدارة بطاقات السياح، ورصد عمليات التحقق، ومتابعة استخدام البطاقة بشكل آني.

الابتكار الخدمي: إصدار بطاقة سياحية موحدة تمكّن السائح من الوصول إلى مجموعة متنوعة من الخدمات السياحية باستخدام بطاقة واحدة، بدلاً من استعمال عدة تذاكر أو اشتراكات منفصلة.

الابتكار التنظيمي: تحسين إدارة الخدمات السياحية من خلال نظام تحقق آلي يسمح بمراقبة الدخول وتنظيم حركة السياح داخل المواقع السياحية.

: المحور الثالث: التحليل الاستراتيجي للسوق

✦1. تحليل المتغيرات الكلية (PESTEL)

التحليل	العامل
العوامل السياسية	• ✓ دعم الاستقرار السياسي للاستثمار في الأنظمة الذكية. • ✗ تأثير سياسات الضرائب والإعفاءات على تكاليف المشروع. • ✗ تأثير سياسات الاستيراد على تكلفة البطاقات وأجهزة التحقق.
العوامل الاقتصادية	• ✗ ارتباط نجاح المشروع بالقدرة الشرائية. • ✓ الطلب مستمر طوال السنة. • ✓ توفر المواد الأولية والإعفاءات يدعم الاستقرار المالي.
العوامل الاجتماعية	• ✓ التحول الرقمي يزيد من تقبل النظام. • ✓ يخدم مختلف الفئات العمرية. • ✓ ارتفاع الوعي بالأمن المعلوماتي يسهل الاستخدام.
العوامل التكنولوجية	• ✓ توفر تقنيات التشفير والبنية التحتية الرقمية. • ✓ إمكانية تطوير تطبيق جوال. • ✓ دمج الذكاء الاصطناعي لتحسين الأداء.
العوامل البيئية	• ✗ المخاطر المحتملة للنظام بسبب انقطاع الشبكة أو ظروف الطقس. • ✓ استخدام بطاقات قابلة لإعادة الاستخدام جزء من الاستدامة.
العوامل القانونية	• ✗ الاحتياجات التي تفرضها قوانين حماية البيانات. • ✓ احترام قوانين العمل المحلية.

▲ تحليل إحصائي مبسط

- ✓ **نسبة العوامل الإيجابية:** تمثل حوالي 65% من مجموع العوامل، مما يدل على وجود بيئة ملائمة لتبني المشروع.
- ✗ **نسبة العوامل السلبية:** تمثل حوالي 35%، وهي مرتبطة أساساً بالجوانب الاقتصادية والقانونية.
- ★ **أهم عامل إيجابي:** التحول الرقمي وتوفر البنية التحتية التكنولوجية.
- ▲ **أهم عامل سلبي:** الاعتماد على الإنترنت والتشريعات المتعلقة بحماية البيانات.
- ✦ **الاستنتاج العام:** البيئة الخارجية تعتبر مشجعة لإطلاق المشروع مع ضرورة التركيز على تقليل المخاطر التقنية والقانونية.

✦ 2- عرض القطاع السوقي

❑ السوق المحتمل:

يهدف مشروع نظام تفعيل البطاقة السياحية الذكية إلى تسهيل استفادة المسافرين من المنحة السياحية من خلال تفعيل البطاقة والتحقق منها رقمياً قبل السفر أو أثناءه، ويتم في ذلك تفعيل البطاقة مسبقًا في بلد الإقامة أو قبل بداية الرحلة، ويتمثل السوق المحتمل في:

- ✔ المكاتب المعتمدة لتسويق البطاقة السياحية.
- ✔ المنصات الرقمية للخدمات السياحية.

❑ السوق المستهدف:

يركز المشروع بشكل خاص على الفئات التالية:

- ✔ الحكومة الجزائرية.
- ✔ البنوك الجزائرية.
- ✔ السياح المحليين المسافرين لأغراض سياحية.
- ✔ الزبائن الذين يفضلون الخدمات الرقمية قبل سفرهم.

وقد اختار المشروع الفئة السابقة لأنها تعتمد على أنظمة الحجز والتخطيط المسبق للرحلات، وتهدف إلى الحصول على حلول رقمية تسهل عملية تفعيل البطاقة السياحية.

✦ 3- قياس شدة المنافسة

1. **حدة المنافسة:**

تُعد حدة المنافسة متوسطة إلى ضعيفة في المرحلة الحالية، نظراً لعدم وجود حلول محلية متخصصة تقدم نظاماً متكاملاً للبطاقة السياحية الذكية. ومع ذلك، يمكن أن تزداد المنافسة مستقبلاً مع توجه المؤسسات المالية والسياحية نحو التحول الرقمي واعتماد تقنيات الدفع والتعريف الذكية.

2. **المنافسون:**

لا يوجد منافسون مباشرون يقدمون نفس الحل المتكامل. ومع ذلك، تُعتبر شركة SATIM من الجهات التي توفر خدمات الدفع الإلكتروني والبطاقات البنكية في الجزائر، لكنها لا تقدم نفس النظام المتكامل الخاص بالسياحة والتنقل الذكي.

أما المنافسون غير المباشرين فيتمثلون في:

- البنوك التي تعتمد على الإجراءات التقليدية لمعالجة ملفات المنحة السياحية.
- وكالات الأسفار التي تقدم خدمات مرافقة للمسافرين دون نظام رقمي متكامل.
- التطبيقات البنكية التي توفر خدمات رقمية محدودة دون التكامل مع بطاقة ذكية أو جهاز تحقق مخصص.

نقاط ضعف هذه الحلول التي يمكن استغلالها:

- بطء الإجراءات الإدارية واعتمادها على المعالجة اليدوية.
- طول مدة انتظار الزبون للحصول على الخدمة.
- غياب التتبع الفوري للبطاقات والمعاملات.
- عدم توفر نظام تحقق ذكي يعتمد على تقنية NFC.
- ضعف التكامل بين مختلف الخدمات الرقمية.

3. **قوة العملاء:**

تتمتع شريحة العملاء بقوة تفاوضية متوسطة، حيث تتوفر بعض البدائل التقليدية، إلا أن المشروع يقدم مزايا إضافية تتمثل في السرعة، سهولة الاستخدام، التتبع الفوري، والأمان المرتفع، مما يعزز جاذبيته لدى العملاء.

4. **قوة الموردين:** حيث يوجد العديد من الموردين المحليين والدوليين، مما يسمح لنا بالتفاوض على الأسعار، حيث يقدمون المكونات الإلكترونية، الشرائح الذكية، وتقنيات الاتصال اللازمة في تصنيع جهازنا.

5. **تهديد المنتجات البديلة:**

يوجد تهديد متوسط من الحلول التقليدية والتطبيقات البنكية الرقمية، إلا أنها لا توفر نفس مستوى التكامل بين البطاقة الذكية، جهاز التحقق، التطبيق المحمول، والمنصة الإلكترونية، مما يمنح المشروع ميزة تنافسية واضحة.

6. **تهديد دخول منافسين جدد:**

يواجه دخول منافسين جدد إلى هذا المجال صعوبات كبيرة، بسبب ارتفاع تكاليف البحث والتطوير، الحاجة إلى خبرات تقنية متقدمة، المتطلبات القانونية والتنظيمية، إضافة إلى ضرورة بناء شراكات مع الجهات السياحية والمالية، مما يشكل عائقًا قويًا أمام المنافسة الجديدة.

✦ 4- الاستراتيجيات التسويقية

يعتمد مشروع البطاقة السياحية الذكية على ثلاث استراتيجيات تسويقية رئيسية:

✝ 3- استراتيجية التركيز:

تعتمد هذه الاستراتيجية على توجيه خدمات المشروع نحو فئات معينة من المستخدمين، مثل:

- ✔ السياح الذين يقومون بالسفر بشكل متكرر.
- ✔ الأشخاص المهتمين بالخدمات الرقمية الحديثة.
- ✔ وكالات الأسفار والشركاء المعتمدين.

ويتم تقديم خدمات مخصصة لهذه الفئات، من بينها:

- ✔ عروض خاصة للمجموعات السياحية.
- ✔ خدمات مميزة للشركاء.
- ✔ واجهات استخدام مخصصة حسب نوع المستخدم.

✦5. تحليل SWOT

نقاط الضعف (Weaknesses)	نقاط القوة (Strengths)
• الاعتماد الكبير على الاتصال بالإنترنت. • ارتفاع تكاليف الصيانة والتحديثات الدورية. • إمكانية حدوث أعطال تقنية مفاجئة. • الحاجة إلى تدريب المستخدمين على استعمال النظام. • محدودية استخدام النظام لدى الأشخاص غير المتمكنين من التكنولوجيا.	• بطاقة مسبقة الدفع بقيمة 750 يورو مصممة لتعزيز سهولة استخدامها من قبل السياح. • تفعيل فوري عند وصول المستخدم إلى المطار أو الحدود من خلال تقنية NFC. • توفير مستوى عالي من أمان بدون تلامس وحماية بيانات المستخدم. • يتيح التطبيق المحمول والمنصة الإلكترونية إدارة رصيد ومتابعة المعاملات. • نظام متكامل يوازن بين البطاقة والجهاز والتطبيق والمنصة.
التهديدات (Threats)	**الفرص (Opportunities)**
• مشاكل اتصال بالإنترنت أو توافق الأجهزة في المطارات. • تغييرات في القوانين المصرفية أو السياحية. • أعطال تقنية تؤثر على تجربة المستخدم. • المنافسة من حلول دفع أخرى وبطاقات سياحية. • مخاطر أمنية/اختراق بيانات البطاقة.	• تزايد الاعتماد على الخدمات الرقمية في القطاعين السياحي والمالي. • زيادة عدد المسافرين المستفيدين من المنحة السياحية سنوياً. • إمكانية عقد شراكات مع البنوك والمطارات ووكالات السفر. • التوسع مستقبلاً نحو خدمات الدفع الإلكتروني والتحقق الرقمي. • الاستفادة من برامج دعم الابتكار والتحول الرقمي.

▲ تحليل SWOT

- ✓ **الاستنتاج العام:** يظهر تحليل SWOT أن المشروع يتمتع بنقاط قوة مهمة، خاصة من حيث التكامل بين مكوناته (بطاقة، جهاز، تطبيق) ومستوى الأمان العالي.
- ★ **استغلال الفرص:** يمكن للمشروع الاستفادة من التوجه المتزايد نحو الرقمنة في القطاعين السياحي والمالي، إضافة إلى إمكانية عقد شراكات استراتيجية مع البنوك والمطارات.
- ✗ **التحديات:** أهم التحديات تتمثل في الاعتماد على الاتصال بالإنترنت وارتفاع تكاليف الصيانة، مما يتطلب حلول تقنية بديلة وخطط دعم مستمرة.
- ▲ **إدارة المخاطر:** يجب التركيز على تقوية جانب الأمن المعلوماتي وتحديث النظام باستمرار لتقليل مخاطر الاختراق أو الأعطال التقنية.

✦6. المزيج التسويقي للبطاقة والجهاز

✦1.6 المنتج

العنصر	جهاز التفعيل	البطاقة الذكية
اللون	ابيض	ذهبي، بنفسجي
الحجم	10 × 6 × 2.5 سم	8.5 × 5.4 × 0.1 سم
الشكل	جهاز إلكتروني بشاشة رقمية ولوحة تحكم	بطاقة بلاستيكية ذكية مع شريحة NFC
التغليف	علبة كرتونية احترافية تحتوي على الجهاز والشاحن ودليل الاستخدام	علبة بلاستيكية شفافة
الشعار		
المميزات التقنية	• قارئ RFID/NFC عالي الدقة • GPS لتحديد الموقع • شاشة عرض تفاعلية • تنبيه صوتي • تحديثات Firmware عن بعد	• تقنية NFC • UID فريد • تشفير AES • تخزين آمن • توافق مع الأجهزة
الجودة	هيكل صناعي متين، مقاوم للغبار، ضمان سنة	مواد PVC مقاومة للخدش والماء
الخدمة	• تفعيل البطاقة السياحية بقيمة 750 يورو عبر جهاز التحقق الذكي. • التحقق من صلاحية البطاقة قبل استخدامها. • إتاحة إمكانية إلغاء أو إعادة تفعيل البطاقة عند الحاجة. • إرسال إشعارات فورية حول حالة التفعيل والاستخدام.	• توفير خدمة التفعيل الفوري للبطاقة عند نقاط الدخول. • دعم عمليات التحقق الأمني من البطاقة. • تحديث النظام وصيانة الجهاز بشكل دوري. • ضمان استمرارية الخدمة وربطها بالمنصة الرقمية.

✦2.6 الترويج- التوزيع -السعر

❧ Price (السعر):

يعتمد المشروع سياسة تسعير قائمة على القيمة المضافة وليس فقط على تكلفة الإنتاج، حيث يوفر:

- ✔ تخفيض التكاليف التشغيلية مقارنة بالمعالجة التقليدية.
- ✔ تسريع عملية التحقق وتفعيل البطاقات في ثوانٍ معدودة.
- ✔ تقليل الأخطاء البشرية وتحسين دقة المعاملات.
- ✔ توفير نظام مبتكر يعتمد على تقنيات NFC والتتبع الذكي.
- ✔ تحسين تجربة المستخدم من خلال التطبيق والمنصة الإلكترونية.

لذلك تم تحديد سعر بيع الجهاز بما يعكس قيمته التقنية والاقتصادية وقدرته على تحقيق وفورات تشغيلية للمؤسسات المستفيدة.

● التوزيع:

- ✔ سيتم توزيع المنتج من خلال شركات متخصصة في توزيع الأجهزة والبطاقات الذكية.
- ✔ سيتم توفير المنتج في منافذ البيع التابعة للشركة.
- ✔ سيتم الدفع عبر وسائل الدفع الإلكترونية أو التحويلات البنكية أو نقدًا حسب طبيعة الزبون.

✝ الترويج:



شكل 4: وسائل الترويج

المحور الرابع: خطة الإنتاج والتنظيم

✦ 1- خطة الإنتاج

✦ 1-1 مراحل عملية الإنتاج



✦ 1-2 اختيار موقع المشروع

الموقع: سيتم تنفيذ المشروع في ورشة عمل مستقلة بمساحة 53 متر مربع.





✦ 3-1 طبيعة الإنتاج

يستند المشروع في مرحلته الأولى على إنتاج شبه صناعي، حيث يشمل:

- تجميع الأجهزة داخليًا داخل مقر المشروع.
- تطوير البرمجيات داخليًا بواسطة فريق التطوير.
- استيراد البطاقات الذكية من موردين متخصصين ومعتمدين.

✦ 4-1 الطاقة الإنتاجية

العنصر	الكمية الشهرية
أجهزة التحقق الذكية	10 إلى 30 جهاز
البطاقات الذكية	800 إلى 1000 بطاقة

العنصر	الكمية السنوية
الأجهزة	120 إلى 360 جهاز
البطاقات الذكية	9600 إلى 12000 بطاقة

✦ 5-1 المواد الأولية اللازمة للإنتاج

المادة	العدد	السعر (دج)	المجموع (دج)
لوحة التحكم ESP32	1	1500	1500
شاشة OLED	1	1200	1200
لوحة مفاتيح	1	350	350
قارئ NFC	1	600	600
بطاقات NFC (ذكية)	30	30	900
وحدة GPS	1	700	700
بطارية	1	600	600
صفارة	1	250	250
هيكل بلاستيكي (3D)	1	5000	5000
أسلاك وتوصيلات	1	600	600
لوحة توصيل	2	240	480
المجموع			**11,280 دج**

✦ 6-1 الموردون الرئيسيون

يتم التزود بالمواد الأولية والتجهيزات من موردين محليين ودوليين متخصصين، ومن أهمهم:

- موردو بطاقات NFC والشرائح الذكية.
- موردو وحدات ESP32 والمكونات الإلكترونية.

- موردو أجهزة GPS وقارئات NFC.
- شركات استضافة الخوادم والحلول السحابية.
- موردو معدات الإعلام الآلي والأجهزة المكتبية.
- موردو الطابعات والمواد البلاستيكية الخاصة بتغليف البطاقات.

✦ 1-7 الموارد البشرية اللازمة

✦ 1-7-1 العمالة المباشرة

الوظيفة	العدد	الراتب الشهري
مطور Stack Full	1	60,000
تقني إلكترونيات	1	60,000
Designer UI/UX	1	45,000
المجموع		**165,000 دج**

✦ 1-7-2 العمالة غير المباشرة

الوظيفة	العدد	الراتب الشهري
محاسب	1	40,000

✦ 1-8 مناصب الشغل التي يخلقها المشروع

يساهم المشروع في خلق مناصب شغل مباشرة وغير مباشرة كما هو موضح في الجدول التالي:

المنصب	العدد
مطور Stack Full	1
تقني إلكترونيات	1
مصمم UI/UX	1
محاسب	1
مسؤول تسويق رقمي	1
مسؤول دعم فني وخدمة العملاء	1
إجمالي المناصب المباشرة	**6**

كما يساهم المشروع في خلق فرص عمل غير مباشرة لدى الموردين وشركات النقل والتوزيع والشركاء التجاريين.

✦ 1-9 الشراكات الرئيسية

يعتمد المشروع على مجموعة من الشراكات الاستراتيجية لضمان نجاح عملية الإنتاج والتسويق، ومن أهمها:

- البنوك الجزائرية المكلفة بتسيير المنحة السياحية.
- المطارات والمنافذ الحدودية لتوفير نقاط التحقق.

- وكالات السياحة والأسفار كشركاء في الترويج للخدمة.
- شركات تطوير البرمجيات والخدمات السحابية.
- شركات الاتصالات لضمان الربط الشبكي والتحديثات.

✦ 10-1 الأثاث ووسائل النقل

العنصر	العدد	السعر	المجموع
مكتب إداري	7	28,000	196,000
كراسي مكتب	10	7,000	70,000
مكيف هواء	3	70,000	210,000
وسيلة نقل (كراء سنوي)	1	72,000	72,000
المجموع			**548,000 دج**

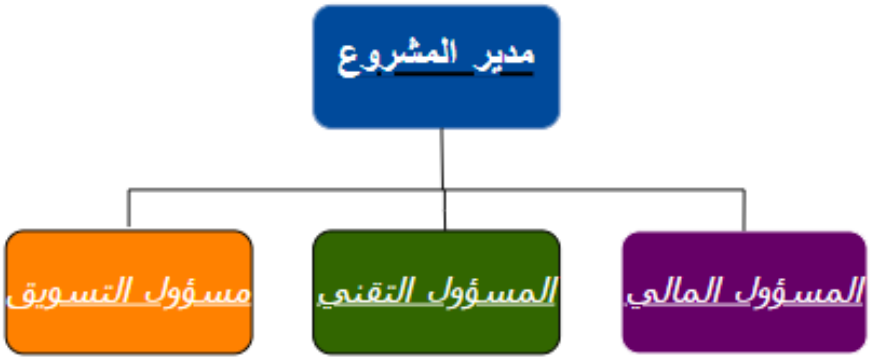
✦ 11-1 المعدات والتجهيزات

المعدة	العدد	السعر	المجموع
قفازات حماية	4	500	2,000
نظارات حماية	5	1000	5,000
خادم (Server)	1	20,000	20,000
مودم إنترنت	1	7,000	7,000
جهاز لحام	1	2,000	2,000
أسلاك لحام	2	800	1,600
كماشات	1	200	200
جهاز قياس الفولت	1	5,500	5,500
طباعة PVC	1	2,000	2,000
طباعة ثلاثية الأبعاد	2	5,000	10,000
UPS (مزود طاقة)	1	12,000	12,000
كاميرات مراقبة	1	15,000	15,000
Laptop تطوير	2	85,000	170,000
Workstation PC	1	90,000	90,000
المجموع			**342,300 دج**

✦ 12-1 التكاليف غير المباشرة

العنصر	القيمة السنوية
راتب المحاسب	480,000
كراء المقر	420,000
إنترنت واستضافة	240,000
كهرباء وصيانة	240,000
مصاريف إدارية	180,000
تسويق وإعلانات	240,000
الأثاث ووسائل النقل	548,000
الإجمالي السنوي	**2,348,000 دج**

✦ 2- التنظيم الداخلي



المحور الخامس: الخطة المالية FINANCIER PLAN

تهدف الخطة المالية إلى تحديد التكلفة الحقيقية لإنتاج جهاز التحقق الذكي عبر توزيع التكاليف المباشرة وغير المباشرة على الإنتاج السنوي.

1- التكاليف الاستثمارية

الأصول	القيمة (دج)
الأثاث ووسائل النقل	548,000
المعدات والتجهيزات	342,300
إجمالي الاستثمارات	**890,300 دج**

2- التكاليف التشغيلية السنوية

البند	القيمة (دج)
المواد الأولية للإنتاج	2,932,800
رواتب العمالة المباشرة	1,980,000
رواتب العمال غير المباشرين	480,000
كراء المقر	420,000
إنترنت واستضافة	240,000
كهرباء وصيانة	240,000
مصاريف إدارية	180,000
تسويق وإعلانات	240,000
إجمالي التكاليف السنوية	**7,260,800 دج**

3- تحديد تكلفة إنتاج الجهاز الواحد

عدد الأجهزة السنوي: 260 جهاز

التكاليف المباشرة السنوية:

- المواد الأولية: 2,932,800 دج
- العمالة المباشرة: 1,980,000 دج

المجموع = 4,912,800 دج

التكاليف غير المباشرة:

- 2,348,000 دج

التكلفة الإجمالية السنوية:

$$7,260,800 \text{ دج}$$

تكلفة الجهاز الواحد:

$$\frac{7,260,800}{260} \approx 27,926 \text{ دج}$$

سعر البيع المقترح: 35,000 دج

تكلفة البطاقة الذكية:

- تكلفة شراء البطاقة: 150 دج
- سعر البيع المعتمد ضمن الجهاز: 280 دج
- هامش الربح لكل وحدة: 130 دج

يُظهر هذا المثال وجود هامش ربح على مستوى المكونات، مما يساهم في تحسين الربحية الإجمالية للجهاز.

السنة	N	N+1	N+2	N+3	N+4	N+5	N+6
عدد الأجهزة المباعة	120	180	240	280	320	340	360
رقم الأعمال من الأجهزة (دج)	4,200,000	6,300,000	8,400,000	9,800,000	11,200,000	11,900,000	12,600,000
إيرادات البطاقات (دج)	2,688,000	2,856,000	3,024,000	3,136,000	3,248,000	3,304,000	3,360,000
رقم الأعمال الإجمالي (دج)	**6,888,000**	**9,156,000**	**11,424,000**	**12,936,000**	**14,448,000**	**15,204,000**	**15,960,000**

جدول 1: توقعات رقم الأعمال خلال السنوات القادمة

4- تقدير عدد الأجهزة المطلوبة

يتم تقدير عدد الأجهزة اعتمادًا على عدد البوابات فقط داخل كل موقع. فالمطارات الدولية تحتوي على عدد كبير من البوابات مقارنة بالمعابر الحدودية، حيث قد يتراوح متوسط البوابات في المطار الواحد بين 10 إلى 30 بوابة دخول وخروج حسب حجم المطار. أما الموانئ والمعابر الحدودية فتحتوي على عدد أقل من البوابات، غالبًا بين 2 إلى 6 بوابات لكل موقع.لذلك يتم حساب العدد الإجمالي للأجهزة عبر جمع متوسط نقاط الخدمة في كل نوع من المواقع لضمان تغطية جميع مراحل عبور المسافرين بشكل دقيق وفعّال.

5- الإيرادات المتوقعة

- 260 جهاز × 35,000 دج = 9,100,000 دج
- بطاقات NFC (تقريباً 9600 إلى 12000 بطاقة × 280 دج) = 2,688,000 إلى 3,360,000 دج
- صيانة = 500,000 دج

الإيرادات الإجمالية = 12,288,000 إلى 12,960,000 دج

6- النتائج المالية

البند	القيمة
الإيرادات	12,288,000 إلى 12,960,000
التكاليف	7,260,800
صافي الربح	**5,027,200 إلى 5,699,200 دج**

تُظهر الدراسة أن المشروع مربح ويحقق هامش ربح جيد مع تكلفة إنتاج واقعية.

✦ 7- خطة الخزينة

تُعد خطة الخزينة من العناصر الأساسية لضمان التوازن المالي للمشروع، حيث تهدف إلى متابعة التدفقات النقدية (المداخيل والمصاريف) بشكل دوري لضمان استمرارية النشاط دون عجز مالي.
تعتمد الخطة على:

- توقع الإيرادات الشهرية الناتجة عن بيع الأجهزة والبطاقات.
- تحديد المصاريف الثابتة مثل الإيجار، الرواتب، والاشتراكات.
- تغطية المصاريف المتغيرة مثل الصيانة والتسويق.
- الحفاظ على سيولة مالية كافية لمواجهة الطوارئ.

كما تسمح خطة الخزينة بتقييم الوضع المالي للمشروع بشكل مستمر واتخاذ قرارات تصحيحية عند الحاجة.

المحور السادس : النموذج الأولي التجريبي

✦ النموذج الأولي للبطاقة وجهاز التحقق



صورة توضيحية 1

البطاقة السياحية الذكية



صورة توضيحية 2

جهاز التحقق الذكي



صورة توضيحية

جهاز الدفع الإلكتروني

✦ الملحق رقم 04: نموذج العمل التجاري

