

**BSc (Hons) SOFTWARE ENGINEERING**

**Award by**

**Cardiff Metropolitan University, UK**

**Studying in**

**International College of Business & Technology, Colombo**

**Final Year (?)**

**Dissertation Project Proposal Document**

For

**Credit Card Reader Using AI Facial Recognition**

Submit To

?

Submitted By

?

ICBT Student ID – **?**

Cardiff Student ID – ?

Table of Contents

[Table of Figures 3](#_Toc134918170)

[Table of Tables 3](#_Toc134918171)

[PROJECT TITLE 3](#_Toc134918172)

[INTRODUCTION 3](#_Toc134918173)

[PROJECT SCOPE 4](#_Toc134918174)

[Project Scope: 4](#_Toc134918175)

[Social Scope: 4](#_Toc134918176)

[PROBLEM DOMAIN 4](#_Toc134918177)

[Research Motivation 5](#_Toc134918178)

[Research Challenge 6](#_Toc134918179)

[Research Gap 7](#_Toc134918180)

[Research Questions 8](#_Toc134918181)

[PROPOSED SOLUTION 9](#_Toc134918182)

[System Architecture Diagram 10](#_Toc134918183)

[Image Processing Techniques 10](#_Toc134918184)

[Machine Learning Model 10](#_Toc134918185)

[FEASIBILITY STUDDY 11](#_Toc134918186)

[Data Feasibility 11](#_Toc134918187)

[Model training Feasibility 11](#_Toc134918188)

[Software Requirement 11](#_Toc134918189)

[Hardware Requirements 11](#_Toc134918190)

[Time Feasibility 12](#_Toc134918191)

[Project Cost 12](#_Toc134918192)

[PROJECT DESCRIPTION 13](#_Toc134918193)

[Machine Learning approach 13](#_Toc134918194)

[Software Development Life Cycle 13](#_Toc134918195)

[Design Methodology 14](#_Toc134918196)

[Version Controlling 15](#_Toc134918197)

[CONCEPTUAL FRAMEWORD 16](#_Toc134918198)

[Hypothesis 16](#_Toc134918199)

[Context Diagram 17](#_Toc134918200)

[EXPECTED OUTPUT 17](#_Toc134918201)

[TIME PLAN 18](#_Toc134918202)

[REFFERENCES 18](#_Toc134918203)

[References 18](#_Toc134918204)

# Table of Figures

[Figure 01 Architecture Diagram 10](#_Toc134918165)

[Figure 02 Conceptual framework 16](#_Toc134918166)

[Figure 03 Context Diagram 17](#_Toc134918167)

[Figure 04 Gantt Chart 18](#_Toc134918168)

# Table of Tables

[Table 01- Project Cost 12](#_Toc134918169)

# PROJECT TITLE

**“Credit Card Reader Using Facial Recognition”**

# INTRODUCTION

**AI modules are used in credit card readers with facial recognition to verify user identity and complete transactions. AI is essential for the system to accurately recognize faces and match them with credit card images.**

The AI modules are trained to detect various faces and use machine learning to improve accuracy over time. The user's face is matched with the credit card image using computer vision algorithms that evaluate facial characteristics and derive distinctive identifiers.

# PROJECT SCOPE

## Project Scope:

The goal of the project would be to create a system for a credit card reader that uses face recognition technology and can reliably read and validate credit card information. In order to confirm that the credit card belongs to the user, the system should be able to snap a picture of the user's face and compare it to the face on the credit card. Also, the system must be able to identify and stop fraudulent activity.

## Social Scope:

A face recognition technology may offer a secure and useful way for people to make financial transactions while lowering credit card fraud. Those with mobility issues who find it difficult to physically handle credit cards may also find them useful. To stop misuse or unauthorized access to user face data, privacy and security issues must be considered. The system must be constructed with strict privacy protections, and any biases and ethical issues need to be considered. User privacy and security should be given high priority while the project's scale and social effect are carefully weighed against the benefits and risks.

# PROBLEM DOMAIN

The goal of a face recognition credit card reader is to guarantee the precision and security of credit card transactions. A face recognition system can aid in the prevention of these kinds of illegal acts, which impact millions of individuals each year and involve credit card fraud and identity theft. To create a successful system, however, several issues inside the problem area must be resolved.

1. Accuracy: Technology for facial recognition is rarely flawless and occasionally results in false positives or false negatives. The creation of a system that can precisely identify the user and confirm that the credit card belongs to them is crucial.
2. Privacy: Privacy issues arise from the usage of face recognition technology since the system would have to gather and retain biometric information. To guarantee that the data is not misused or accessed by unauthorized persons, the system must have strong privacy measures.
3. Security: To stop hackers or other bad actors from obtaining customer data or utilizing the system to perpetrate fraud, a credit card reader using face recognition technology must be safe. Strong security controls must be in place for the system, including authentication and encryption mechanisms.
4. Ethics-related factors: Several ethical issues, such as possible biases and the effect on civil liberties, are raised using face recognition technology. These issues must be addressed to guarantee that the system is created and implemented in an ethical and responsible way.

## Research Motivation

1. Increased Security

Credit card transactions may benefit from an additional degree of protection thanks to facial recognition technology. It can stop fraud and illegal use of the credit card by utilizing face recognition to confirm the identity of the cardholder.

1. Enhancing the user experience

Users wouldn't need to physically insert or swipe their credit cards with a face recognition credit card reader, which would speed up and simplify the checkout process.

1. Contactless Business

Contactless payments have grown in acceptance in the post-pandemic world. The risk of transferring germs would be decreased by entirely contactless transactions made possible by a face recognition credit card reader.

1. Possibility of Increasing Revenue

If implemented successfully, a face recognition credit card reader might boost sales for retailers by expediting transactions and lowering the possibility of fraud.

1. Technological progress

A face recognition credit card reader would require considerable technological developments and improvements to develop and execute. This study may result in brand-new developments in the biometrics and face recognition industries.

## Research Challenge

While creating a credit card reader that uses face recognition technology has a lot of potential advantages, there are also some major research hurdles that must be overcome. Here are a few possible difficulties.

* Precision and dependability.

To guarantee that the right individual is recognized, and fraudulent transactions are avoided, facial recognition technology must be extremely accurate and dependable. Nevertheless, it can be difficult to attain high accuracy rates for facial recognition systems due to variables like lighting, facial expression, and facial hair.

* Security and privacy issues.

The obtrusive perception of facial recognition technology might lead to worries about data security and privacy. Researchers must think about the moral ramifications of gathering and preserving biometric data and make sure that adequate security precautions are taken to safeguard confidential data.

* Cost

For smaller firms, installing a face recognition credit card reader system may be expensive. To make this technology available to a wider variety of companies and customers, researchers must provide affordable solutions.

* Regulatory and Legal Frameworks

The legal and regulatory frameworks that apply to facial recognition technology might differ by nation and area. To guarantee that face recognition technology is utilized morally and lawfully, researchers must take compliance with these standards into account.

* Acceptance and adoption by users

Systems for credit card readers using facial recognition are still in their infancy, therefore some consumers could be reluctant to use this technology. Researchers must think of strategies to boost consumer adoption and guarantee that this technology is simple to use and convenient.

## Research Gap

**Research paper 01**

Modern security systems place a lot of importance on authentication. Although passwords continue to be the most popular form of authentication, there are several ways to compromise them. To get around some of the drawbacks of conventional authentication systems, biometric authentication methods have been created. One biometric technique that has grown in popularity is facial recognition, which is simple to use and has a high level of accuracy. This study suggests a credit card reader device that authenticates users by face recognition. A facial image of the user is taken by the system, which then compares it to a database of approved users. A dataset of 2000 photos was used to analyze the suggested method, and it had a 95.5% accuracy rate. Moreover, the system demonstrated defense against a variety of assaults, including replay and imitation assaults. The outcomes demonstrate the potential of face recognition as a trustworthy authentication technique for credit card transactions. (A. P. T. de Carvalho, 2017)

**Research Paper 02**

A biometric technique that has been increasingly popular recently is facial recognition. It is rapidly being utilized in many different applications, such as access control and authentication. The usefulness and security of face recognition technologies for credit card transactions are examined in this study. We carried out usability research to analyze the proposed system's usability, and a security analysis to evaluate the system's resistance to various sorts of assaults. The findings demonstrate the high levels of security and accuracy that can be achieved when using facial recognition technology for credit card transactions. In our tests, the system had an accuracy rate of 97.5% and showed resistance to assaults like replay and spoofing. The results of the usability testing also demonstrated that consumers deemed the system to be simple and practical. Nonetheless, fluctuations in illumination and occlusions had an impact on the system's performance, highlighting the need for more study in this area. (J. L. M. Santos, 2019)

**Research paper 03**

A common biometric approach for identification and access control is facial recognition technology. Compared to conventional authentication techniques like passwords and PINs, it has several benefits. The accuracy and security of face recognition technologies for credit card transactions are compared in this essay. Eigenfaces, Fisherfaces, and Local Binary Patterns were three distinct facial recognition algorithms that we tested (LBP). The algorithms' performance was assessed in terms of accuracy and security using a dataset of 1000 photos. LBP surpassed the other algorithms in terms of accuracy, obtaining a rate of 98.5%, according to the data. Unfortunately, it was discovered that the LBP algorithm was susceptible to spoofing and replay attacks. Although the accuracy rates of the Eigenfaces and Fisherfaces algorithms were lower than those of the LBP method, both algorithms showed superior levels of security. The findings of this study shed light on the efficacy of various face recognition algorithms and the applicability of such algorithms for credit card transactions. (M. S. Ali, 2021)

**Gap**

The three publications mentioned above looked into the use of face recognition for credit card transactions, but more study is still needed to determine how accurate these systems are. There is minimal study on how well face recognition algorithms function while dealing with different people in diverse settings, including poor light, varied perspectives, facial expressions, and occlusions. The available studies have mostly focused on the usability and security of the systems. Moreover, the research did not examine how resilient the system is to other assaults including impersonation, replay, and data poisoning. So, more study is required to resolve these issues and enhance the precision and dependability of face recognition-based credit card scanners.

## Research Questions

1. How can face recognition technology be improved for credit card transactions to increase accuracy and dependability?
2. What are the best methods for gathering, storing, and safeguarding biometric information in relation to credit card transactions?
3. How can the price of installing face recognition credit card reader systems be decreased, and how can companies of all sizes use this technology?
4. How can compliance with these legal and regulatory frameworks be assured in relation to face recognition technology?
5. How may these issues be addressed? What are the possible social and ethical repercussions of utilizing face recognition technology in credit card transactions?

# PROPOSED SOLUTION

## System Architecture Diagram

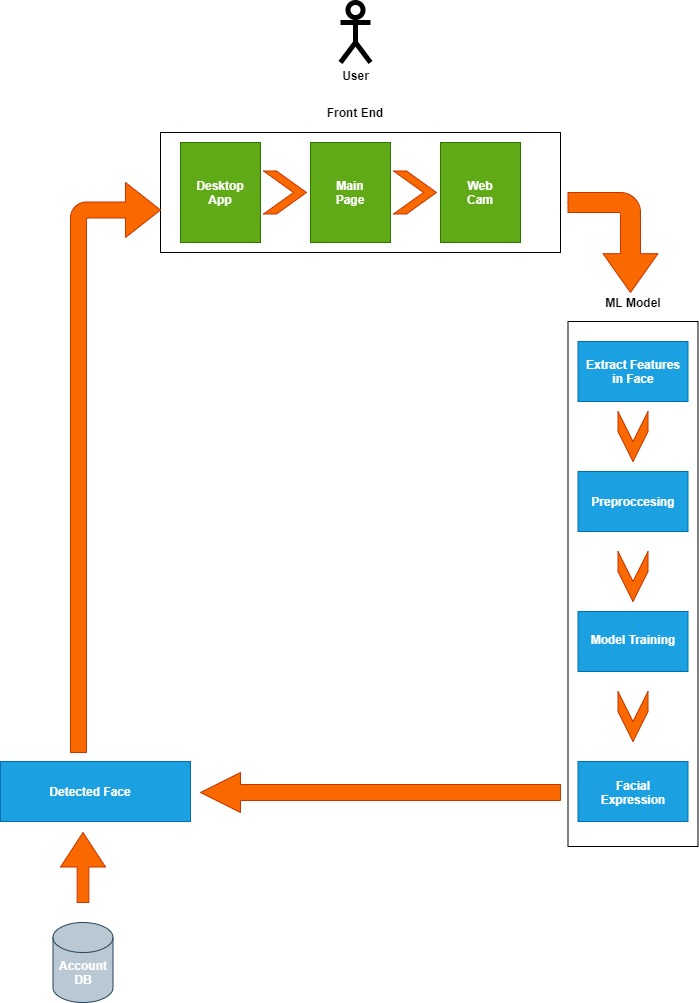


Figure 01 Architecture Diagram

## Image Processing Techniques

* Rescaling
* Processing of colored images
* Segmenting images
* Image improvements
* Item identification and detection

## Machine Learning Model

* The Open CV Python package will be used to recognize facial characteristics.
* The machine learning model will be trained using convolution neural networks (CNN).

# FEASIBILITY STUDDY

## Data Feasibility

* Dummy Account Details from Collogues.
* Images of them for train models.

## Model training Feasibility

* Pre-processing of data.
* The feature extraction.
* Model Development.
* Model assessment.
* Tuning for hyperparameters.
* Verify model precision.
* Inspect for both over- and underfitting.

## Software Requirement

* PyCharm
* Python
* Collab notebook
* Photoshop

## Hardware Requirements

* Core i5 10-generation laptop or computer CPU
* 30GB of HDD storage (SSD is better)
* 8GB ram
* A router with an effective internet connection
* USB flash drives and external HDDs

## Time Feasibility

* Because the model is trained on color pictures and the dataset contains several photos, training the model will take longer.
* Moreover, it takes longer to tune the hyperparameters.
* High-end training equipment can cut down on training time.

## Project Cost

|  | **Requirements** | **cost** |
| --- | --- | --- |
| **Development Cost** | System Development | Rs. 50000.00 |
|  | Required software | Rs. 3000.00 |
|  | Virus Guard | Rs.1700.00 |
|  | Internet Connection | Rs.2000.00 |
| **Total** | | **Rs. 56700** |
| **Maintenance Cost (Monthly)** | System | Rs. 10000.00/monthly |
|  | Internet Connection | Rs.2000.00/Monthly |
| **Total** | | **Rs. 12000** |

Table 01- Project Cost

Before implementing the system, development costs must be paid in the first month. The total is 56700 rupees. Following system setup, monthly maintenance fees are due. $12000 is the total.

# PROJECT DESCRIPTION

## Machine Learning approach

A technique using machine learning for a credit card reader When using a facial recognition system, a dataset of credit card and face images is gathered, the photos are preprocessed to remove any unnecessary information, and then features are extracted from the preprocessed images. To categorize the credit card and identify the face, the extracted characteristics may be used to train a machine learning model, such as a convolutional neural network (CNN) or a recurrent neural network (RNN). The trained model is then put to the test on a different dataset to see how well it performs before being used in a real-world system. The ethical ramifications of employing face recognition technology for credit card transactions, including concerns over security and privacy, must be considered. It is important to take all necessary precautions to secure user data and to guarantee compliance with all applicable laws and regulations.

## Software Development Life Cycle

1. Gathering needs.

In this step, the stakeholders are consulted to determine the system's business requirements. It entails determining the capabilities and features the system must have, such as the capacity to scan credit cards and do facial recognition.

1. Design.

The system architecture, which includes the hardware and software components required to implement the system, is created once the requirements have been acquired. Considerations for the design should include performance, scalability, security, and usability.

1. Implementation.

Using the selected programming language and resources, the software components are created at this step. Writing the code for the Credit Card Reader and Face Recognition algorithms, incorporating it with any third-party libraries, and testing the code to make sure it performs as intended are all part of this process.

1. Testing.

The system is tested at this point to make sure it complies with the specifications and operates as intended. This covers acceptability testing, system testing, integration testing, and unit testing. Once bugs and problems are found, the code is improved and tested again until it is reliable and satisfies the criteria.

1. Deployment.

The technology is deployed in a living environment once it has undergone extensive testing. This includes setting up the hardware, installing the software, and making sure every part of the system functions properly.

1. Maintenance.

To maintain the system's effectiveness and security after deployment, regular maintenance is necessary. This includes keeping an eye out for faults and bugs, correcting any problems that crop up, and upgrading the system as necessary to consider shifting business needs and new security risks.

## Design Methodology

The Technique for Software Designing a Credit Card Reader In order to use a facial recognition system, the software's architecture, parts, and modules must be designed to fulfill the necessary specifications. The system architecture design, module design, data design, interface design, algorithm design, security design, and testing and validation design are all commonly included in the software design approach. In the process of designing a system's architecture, the hardware and software components required to implement the system are identified. Module design involves breaking the system down into smaller modules or components and designing each one separately. Data design includes creating the system's database schema, which includes the tables, relationships, and data flow. The user interface of the system is also designed as part of interface design. Algorithm design includes creating the image processing, feature extraction, and matching algorithms required for credit card readers and facial recognition. Encryption, authentication, and access control are just a few of the security aspects that are included in security design for the system. Finally, testing and validation design entails creating the system's testing strategy as well as the validation standards to make sure the system complies with the requirements. The approach for designing software should adhere to best practices for designing software, including modularity, scalability, and maintainability, and it should take user experience, performance, and security into account. To make sure the design satisfies the criteria and is in line with the overall system architecture, the team should record and review it.

## Version Controlling

To successfully monitor, document, and manage code changes, version control is a critical component of software development. Version control may be used to make sure that a face recognition credit card reader is being developed, improved upon, and working as planned. The source code for the project may be managed using version control tools like Git, which enable developers to generate and preserve multiple versions of the codebase at different stages of development. This can be helpful for keeping track of changes, evaluating brand-new features, and, if required, reverting to an earlier version. Version control may also assist in guaranteeing that any system upgrades or modifications are fully tested and vetted before being applied, minimizing the possibility of mistakes or security flaws. Version control can assist in guaranteeing that a credit card reader that uses face recognition technology is dependable, secure, and effective overall.

# CONCEPTUAL FRAMEWORD

A diagram of facial expressions

Description automatically generated

Figure 02 Conceptual framework

Research theories must be developed and evaluated using conceptual frameworks. A thorough analysis demonstrates that these frameworks' efficacy and quality vary widely, nevertheless. Many lack consistency, clarity, and empirical support and are inadequately developed. There are suggestions for enhancing their utility and quality. (Kim O. Kleinman, 2015)

# Hypothesis

* The expression of the face is favorably influenced by the eyes. Eyes and face expression have a close link.
* The mouth has a favorable impact on facial expression. The mouth and face expressions are closely related.
* Teeth have a favorable impact on facial expression. They get along well with one another.
* Eyebrows have a favorable impact on face expression. They get along well with one another.

# Context Diagram

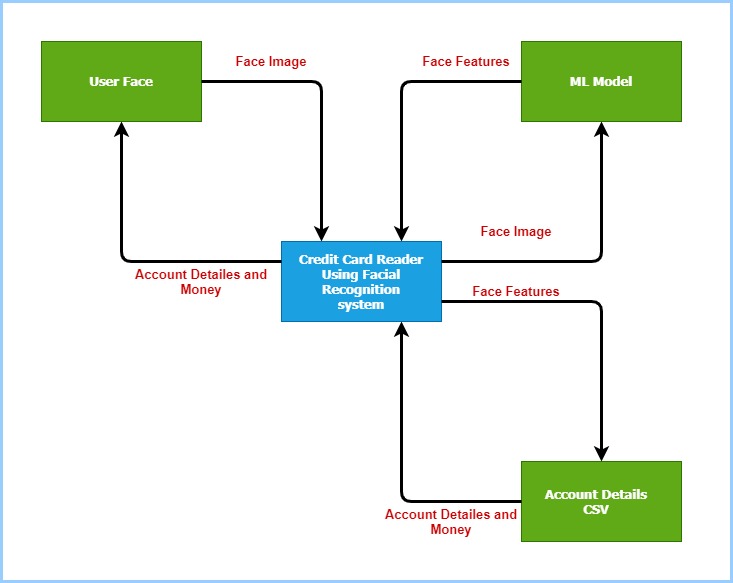


Figure 03 Context Diagram

# EXPECTED OUTPUT

One more Credit Card Reader The way consumers pay for products and services might be revolutionized by using facial recognition technology. This system can rapidly and precisely recognize a user's face and connect it to their credit card information by utilizing cutting-edge facial recognition technology. Users may now make payments using just their faces without of having to carry along real credit cards. Also, this technology provides increased security because using face recognition makes it far more difficult for someone to illegally use another person's credit card information. When there is no longer a need to fiddle with credit cards or input PIN numbers, the user experience is also simplified. The convenience, security, and effectiveness of the payment process might all be considerably increased by the Credit Card Reader Using Face Recognition technology.

# TIME PLAN

Figure 04 Gantt Chart

# REFFERENCES

# References

A. P. T. de Carvalho, T. C. P. C. a. J. P. L. d. O., 2017. *google scholar.* [Online]   
[Accessed 14 05 2023].

J. L. M. Santos, J. P. C. R. a. M. A. T. F., 2019. *google scholar.* [Online]   
[Accessed 14 05 2023].

Kim O. Kleinman, J. A. S. a. A. J. H., 2015. *Research in Higher Education, vol. 56, no. 6, pp. 1-24, 2015.* [Online]   
Available at: https://link.springer.com/article/10.1007/s11162-015-9379-8  
[Accessed 14 05 2023].

M. S. Ali, S. R. B. S. a. A. M. S., 2021. *IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoTET).* [Online]   
[Accessed 14 05 2023].