VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY

An Autonomous Institute Affiliated to University of Mumbai
Department of Computer Engineering

Project Report on

Remote Access Control to Sensitive Areas using Crypto Cards

In partial fulfilment of the Fourth Year, Bachelor of Engineering (B.E.) Degree in Computer Engineering at the University of Mumbai Academic Year 2023-24

Submitted by
Figo Cardozo - D17A/08
Om Madat - D17A/38
Vansh Pahuja - D17A/50
Drishti Samvedi - D17B/63

Project Mentors
Dr. Mrs. Gresha Bhatia
Mrs. Abha Tewari

(2023-24)

VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY
An Autonomous Institute Affiliated to University of Mumbai
Department of Computer Engineering

Certificate

This is to certify that ***Figo Cardozo (D17A/08), Om Madat (D17A/38), Vansh Pahuja(D17A/50), Drishti Samvedi (D17B/63)*** of Fourth Year Computer Engineering studying under the University of Mumbai have satisfactorily completed the project on "***Remote Access Control to Sensitive Areas using Crypto Cards***" as a part of their coursework of PROJECT-II for Semester-VIII under the guidance of their mentor ***Dr. Mrs. Gresha Bhatia and Mrs. Abha Tewari*** in the year 2023-24 .

This project report entitled ***Remote Access Control to Sensitive Areas using Crypto Cards*** by ***Figo Cardozo, Om Madat, Vansh Pahuja, Drishti Samvedi*** is approved for the degree of ***B.E. Computer Engineering***.

Programme Outcomes	Grade
PO1,PO2,PO3,PO4,PO5,PO6,PO7, PO8, PO9, PO10, PO11, PO12 PSO1, PSO2	

Date:
Project Guide:

Dr. Mrs. Gresha Bhatia Mrs. Abha Tewari

टाटा मूलभूत अनुसंधान संस्थान
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
होमी भाभा रोड, कोलाबा, मुंबई – ४०० ००५.
Homi Bhabha Road, Colaba, Mumbai - 400 005.
परमाणु ऊर्जा विभाग की स्वायत्त संस्था
भारत सरकार एवं समविश्वविद्यालय
An Autonomonus Institution of the Department of Atomic Energy
Government of India and Deemed University

दूरभाष / Telephone : +91 22 2278 2000
फैक्स / Fax : +91 22 2280 4610 / 11
वेबसाईट / Website : www.tifr.res.in

Date: 05/8/2023

Letter of Permission

This is to certify that following Final year students of Department of Computer Engineering of Vivekanand Education Society's Institute of Technology, Chembur, are working on a TIFR project titled "**Remote Access Control**", under the guidance of **Dr.Gresha Bhatia and Mrs. Abha Tewari** for the academic year 2023-24.

1. **Figo Cardozo**
2. **Drishti Samvedi**
3. **Vansh Pahuja**
4. **Om Madat**

We will provide all technical assistance to students required during the completion of the project. The progress seminars and meetings will be regularly conducted to take feedback.

Dr. Shashikant Dugad,
Professor, Department of High energy Physics,
Tata Institute of Fundamental Research, Mumbai.

Project Report Approval
For
B. E (Computer Engineering)

This project report entitled ***Remote Access Control to Sensitive Areas using Crypto Cards*** by ***Figo Cardozo, Om Madat, Vansh Pahuja, Drishti Samvedi*** is approved for the degree of ***B.E. Computer Engineering***.

Internal Examiner

External Examiner

Head of the Department

Principal

Date:
Place:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

---	---
(Figo Cardozo - D17A/08)	(Om Madat - D17A/38)
---	---
(Vansh Pahuja - D17A/50)	(Drishti Samvedi - D17B/63)

Date:

ACKNOWLEDGEMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to the Deputy Head of Department **Dr. (Mrs.) Gresha Bhatia** and Assistant Professor **Mrs. Abha Tewari** for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions.

We are deeply indebted to the Head of the Computer Department **Dr. (Mrs.) Nupur Giri** and our Principal **Dr. (Mrs.) J. M. Nair,** for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement several times.

Computer Engineering Department

COURSE OUTCOMES FOR B.E PROJECT

Learners will be,

Course Outcome	Description of the Course Outcome
CO1	Able to apply the relevant engineering concepts, knowledge and skills towards the project.
CO2	Able to identify, formulate and interpret the various relevant research papers and to determine the problem.
CO3	Able to apply the engineering concepts towards designing solutions for the problem.
CO4	Able to interpret the data and datasets to be utilised.
CO5	Able to create, select and apply appropriate technologies, techniques, resources and tools for the project.
CO6	Able to apply ethical, professional policies and principles towards societal, environmental, safety and cultural benefit.
CO7	Able to function effectively as an individual, and as a member of a team, allocating roles with clear lines of responsibility and accountability.
CO8	Able to write effective reports, design documents and make effective presentations.
CO9	Able to apply engineering and management principles to the project as a team member.
CO10	Able to apply the project domain knowledge to sharpen one's competency.
CO11	Able to develop a professional, presentational, balanced and structured approach towards project development.
CO12	Able to adopt skills, languages, environment and platforms for creating innovative solutions for the project.

Index

Chapter No.	Title	Page No.
	Abstract	12
1	**Introduction**	13
	1.1 Introduction	13
	1.2 Motivation	13
	1.3 Problem Definition	14
	1.4 Existing Systems	14
	1.5 Lacuna of the Existing Systems	14
	1.6 Relevance of the Project	15
2	**Literature Survey**	16
	A. Brief Overview of Literature Survey	16
	B. Related Works	16
	2.B.1 Articles Referred	16
	2.B.2 Interaction with Industry Experts	17
	2.1 Research Papers Referred	18
	a. Abstract of the Research Paper	
	b. Inference Drawn	
	2.2 Patent Search	25
	2.3 Inference Drawn	26
	2.4 Comparison with the Existing System	27
3	**Requirement Gathering for the Proposed System**	28
	3.1 Introduction to Requirement Gathering	28
	3.2 Functional Requirements	28
	3.3 Non-Functional Requirements	29
	3.4 Hardware, Software, Tools and Techniques utilised	30
	3.5 Constraints	33
4	**Proposed Design**	34

	4.1 Block Diagram of the System 4.2 Modular Diagram of the System 4.3 Detailed Design a. Data Flow Diagram b. System Design c. ER Diagram 4.4 Project Scheduling and Tracking using Gantt Chart	34 35 36 36 38 39 40
5	**Implementation of the Proposed System** 5.1 Methodology employed for Development 5.2 Algorithms and Flowcharts for the Respective Modules developed	41 41 42
6	**Testing of the Proposed System** 6.1 Introduction to Testing 6.2 Types of Tests considered 6.3 Various Test Case Scenarios considered 6.4 Inference Drawn from the Test Cases	46 46 46 46 48
7	**Results and Discussions** 7.1 Screenshots of User Interface (UI) for the Respective Module 7.2 Performance Evaluation Measures 7.3 Input Parameters considered 7.4 Graphical and Statistical Output 7.5 Comparison of Results with Existing Systems 7.6 Inference Drawn	49 49 54 56 56 56 56
8	**Conclusion** 8.1 Limitations 8.2 Conclusion 8.3 Future Scope	58 58 58 59
	References	60
	Appendix a. Patent Published	62 62

	b. Project Review Sheet c. Competition Certificates	63 64

List of Figures

Figure No.	Heading	Page No.
2.1	Article on Multi-Factor Authentication	16
2.2	Article on Importance of Multi-Factor Authentication	17
4.1	Block Diagram	34
4.2	Modular Diagram of Smart Card Module	35
4.3	Level 0 DFD	36
4.4	Level 1 DFD	37
4.5	Level 2 DFD	38
4.6	System Design	38
4.7	ER Diagram	39
4.8	Gantt Chart of the system	40
5.1	Flowchart of Steps for Registration of User	43
5.2	Flowchart of Steps for Authentication of User	44
7.1	Landing Page of Registration	49
7.2	Form to enter the personal details	49
7.3	Capture your face	50
7.4	Record your voice	50

7.5	Connect NFC Smart Card Reader and place Card on it	50
7.6	Data successfully stored in the card	51
7.7	Registration Successful	51
7.8	Landing Page for Authentication	51
7.9	Tap your card on NFC Smart Card Reader	52
7.10	Card details successfully read	52
7.11	Enter PIN after tapping your card	53
7.12	Face Authentication	53
7.13	Blink eyes for given number of times	53
7.14	After successful face authentication, proceed for voice authentication	53
7.15	Record your voice by saying the given phrase	54
7.16	Access granted if all factors match	54

List of Tables

Table No.	**Heading**	**Page No.**
2.1	Comparison with Existing System	27

Abstract

Traditional access control systems often suffer from security vulnerabilities and logistical challenges, especially when granting access to high-security zones. In this project, we design and implement a novel system that leverages the capabilities of a crypto card to enhance access control measures while ensuring data integrity and confidentiality. The proposed project aims to create a secure remote access control system for sensitive areas. It plans to achieve this goal by leveraging smart card technology and cryptographic techniques along with face and voice recognition. Smart cards act as secure tokens, holding unique credentials for authorized users. Cryptography, on the other hand, will ensure the confidentiality and integrity of data exchanged during the access process. By combining these two technologies, the project seeks to establish a robust and reliable system that allows only authorized individuals to remotely access sensitive areas. This will significantly enhance security measures, reducing the risk of unauthorized access and potential security breaches. The integration of smart cards and cryptography will provide a multi-layered defense mechanism, adding an extra level of protection against potential threats and unauthorized users. Overall, the implementation of this system will contribute to safeguarding valuable assets and sensitive information within the designated areas.

Chapter 1: Introduction

1.1 Introduction

Remote access control plays a crucial role in maintaining the security and integrity of sensitive areas within diverse industries, ranging from corporate offices to research facilities and data centres. However, the conventional access control systems used in these environments often depend on passwords or keycards, leaving them susceptible to various security risks. One of the major vulnerabilities of password-based systems is the potential for password breaches or leaks, either through hacking attempts or social engineering attacks. These weaknesses expose organisations to significant security threats and potential breaches of valuable information. To counter these limitations and ensure a more robust and reliable approach to remote access control, the project advocates the implementation of smart cards and cryptographic techniques. Smart cards serve as secure tokens that store unique credentials for each user, making it significantly more challenging for unauthorised individuals to gain access to sensitive areas. The introduction of cryptographic techniques further strengthens the security of the system by encrypting data exchanged during the authentication process. Moreover, the integration of smart cards and cryptography promises a more user-friendly experience for legitimate users, streamlining the authentication process and enhancing overall operational efficiency.

1.2 Motivation

The motivation for implementing a remote access control system to sensitive areas using crypto cards is rooted in the fundamental need to enhance security, streamline access management, and safeguard critical assets, reducing human error, improving access control, enhancing auditability and accountability, cost efficiency, scalability, leveraging technological advancements, deterring unauthorised access, and protecting sensitive data. Crypto cards offer a more secure and tamper-resistant means of verifying a user's identity, providing a robust audit trail, and reducing the need for frequent reissue of access credentials. They also offer cost savings compared to traditional key-based systems, making them a cost-effective solution for organisations growing or evolving. The project aims to establish a robust and efficient means of controlling access to sensitive areas, ultimately safeguarding critical assets and information.

1.3 Problem Definition

To create a comprehensive access management system that combines PINs, smart card technologies, facial recognition, and voice recognition to deliver a secure, user-friendly solution. The existing password-based security has vulnerabilities that need to be resolved. This project aims to tackle issues related to password security flaws, enhance user authentication through multi-factor authentication methods, ensure robust data protection, and prioritise user comfort. The goal is to create a holistic access management system that not only strengthens security but also improves the overall user experience, addressing the growing need for advanced and reliable access control in modern environments.

1.4 Existing Systems

Existing key card access systems, widely utilized in commercial and residential settings, offer convenience and security, yet they come with notable limitations. Traditional key card systems, reliant on magnetic stripe or RFID technology, are vulnerable to unauthorized duplication or cloning, compromising security. Moreover, these systems require physical cards, which can be misplaced or stolen, leading to access issues and potential breaches. Biometric key card systems, integrating fingerprint or iris recognition, enhance security by adding a unique biological identifier, but they can be costly to implement and may encounter accuracy issues, particularly in environments with varying conditions. Additionally, biometric data storage raises privacy concerns and regulatory compliance challenges, posing ethical dilemmas for organizations. Furthermore, all key card systems are susceptible to technological obsolescence, necessitating periodic upgrades to maintain effectiveness and compatibility with evolving security standards. Thus, while key card access systems offer practicality, their limitations underscore the need for continuous innovation in access control technology.

1.5 Lacuna of the Existing Systems

The concept of a Touchless Attendance System called "Pehchaan" that relies on face and voice recognition without cryptographic measures raises several significant security concerns and vulnerabilities. These include data interception, data tampering, unauthorised database access, privacy concerns, spoofing attacks, data integrity, data retention risks, unauthorised access, and lack of audit trails. Without cryptography, data transmitted between users and the attendance system could be intercepted by malicious actors, leading to compromised

biometric data and attendance records. Cryptography ensures data integrity by making it difficult to tamper with data unnoticed. It also helps limit unauthorised database access, protects privacy by preventing unauthorised access to biometric templates and attendance records, and helps detect and prevent spoofing attacks. Cryptography also contributes to the creation of comprehensive audit trails, enhancing accountability and security.

1.6 Relevance of the Project

Remote Access Control to Sensitive Areas using Crypto Cards is highly relevant in today's rapidly evolving digital landscape. It addresses critical security concerns while enhancing user convenience. With cyber threats becoming increasingly sophisticated, the need for multi-factor authentication, like facial and voice recognition, is paramount in protecting sensitive information. Furthermore, the project addresses the shortcomings of traditional password-based systems, which are vulnerable to breaches. By integrating multiple authentication methods and prioritising data protection, it offers a comprehensive solution for access management. In an era where data privacy and security are paramount, this project contributes significantly to safeguarding critical assets, data, and ensuring user-friendly yet robust access control systems.

Chapter 2: Literature Survey

A. Brief Overview of Literature Survey

A literature survey is a thorough summary of earlier studies on a subject. The literature survey examines scholarly books, journals, and other sources that are pertinent to a particular field of study. With respect to the proposed work, the literature survey comprises a number of research papers and various articles that were referred to during the study of the project. It also comprises Interaction with Industry Experts of Tata Institute of Fundamental Research (TIFR). The details of the same are mentioned below.

B. Related Works

2.B.1 Articles referred

1) Source:

https://www.globalknowledge.com/us-en/resources/resource-library/articles/the-three-types-of-multi-factor-authentication-mfa/

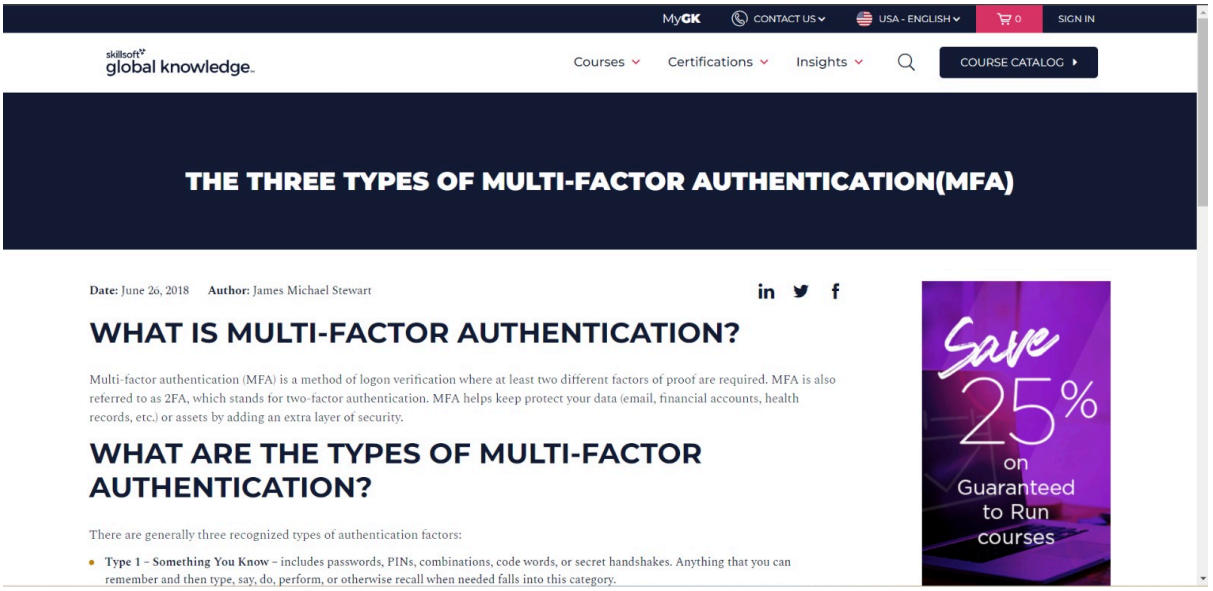

Figure 2.1: Article on Multi-Factor Authentication

Inference: Multi-factor authentication (MFA) is a method of login verification that requires at least two different factors of proof. There are three types of authentication factors: Type 1, Something You Know (passwords, PINs, combinations, code words, secret handshakes),

Type 2, Something You Have (physical objects, token devices, and human body parts), and Type 3, Something You Are (fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification). MFA is preferred as it is more difficult for an intruder to overcome.

2) Source:

https://news.uark.edu/articles/66470/the-importance-of-multi-factor-authentication

Figure 2.2: Article on Importance of Multi-Factor Authentication

Inference: Multi-factor authentication (MFA) is a security method that requires users to enter their credentials multiple times to access their account. It consists of five factors: something known (username and password), something they carry (physical item), something they are (biometrics), something they are (geo location), and something they do (keystroke patterns). Enabling MFA ensures unauthorized users cannot access your account or information without the codes sent directly to your device, email, or phone number. Enabling MFA increases the security of your accounts and information. Ensuring your security information and settings is crucial, and October is National Cybersecurity Awareness Month.

2.B.2 Interaction with Industry Experts

As our project titled 'Remote Access Control to Sensitive Areas using Crypto Card' is in collaboration with **'Tata Institute of Fundamental Research'**, we had an opportunity to interact with Dr. Shashi Dugad who works at TIFR. He provided us with a clear insight of the project and guided us on how to start with the project. From then, after every two or three

weeks, we had an interaction with Shashi sir, to show the implementation of what we had done. He evaluated our work and told us the further things we need to perform. Overall, Shashi sir acted like a guiding light for us.

2.1 Research Papers Referred

1. **Title:** A Novel MQTT Security Framework In Generic IoT Model, Patel, C. and Doshi, N., "A novel MQTT security framework in generic IOT model", 2020, ISSN International conference. Available at: https://www.sciencedirect.com/science/article/pii/S1877050920311297

   Abstract: The Internet of Things (IoT) has revolutionized various aspects of human life, including healthcare, power distribution, agriculture, and industry 4.0. Smart health care technologies like wearable devices have transformed healthcare, while smart grids and smart meters have enabled the distribution of surplus renewable energy. IoT has also improved agriculture by enabling farmers to identify fertilizer needs, pesticide quality, and land moisture using moisture and fertility sensors. IoT uses lightweight communication protocols like MQTT (Message Queuing Telemetry Transport), COAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), and REST (Representational State Transfer) to simplify and speed up communication. The MQTT protocol, which uses TCP as an underlying transport layer, is the most famous protocol in IoT communication at the application layer. However, challenges in securing devices from physical and logical attacks, such as device authentication, resource access control, and data security over insecure channels, remain. This chapter provides an in-depth security survey of IoT-based industry 4.0.

   Inference: IoT has transformed healthcare, energy distribution, and agriculture. MQTT is a key communication protocol in IoT. Security challenges, including device protection and data security over insecure channels, are notable concerns in IoT-driven industry 4.0.

2. **Title:** An Efficient and Practical Smart Card Based Anonymity Preserving User Authentication Scheme for TMIS using Elliptic Curve Cryptography, Amin, R. *et al.* "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography" , 2015 , Springer. Available at: https://link.springer.com/article/10.1007/s10916-015-0351-y

   Abstract: In the last few years, numerous remote user authentication and session key agreement schemes have been put forward for Telecare Medical Information System, where the patient and medical server exchange medical information using the Internet. The scheme is designed to be resistant to attacks and has been validated through simulation using Automated Validation of Internet Security Schemes and Applications software. The performance comparison shows that the proposed scheme has lower communication costs than existing schemes and nearly equal computation cost. The scheme is efficient in terms of different security attacks, provides efficient login, mutual authentication, session key agreement, verification, password update phases, and password recovery.

   Inference: The paper introduces a secure medical system for patients to share data with doctors through a trusted server on an unsecured network. It resists attacks, offers cost-efficient communication, and effectively manages login, authentication, key agreement, verification, password updates, and recovery, making it a robust and practical solution for medical data exchange.

3. **Title:** Elliptic Curve Cryptography based Security Framework for Internet of Things(IoT) Enabled Smart Card , T. D. Premila Bai, K. M. Raj and S. A. Rabara, "Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card", 2017, World Congress on Computing and Communication Technologies (WCCCT). Available at: https://ieeexplore.ieee.org/document/8074489

   Abstract: People across the world use smart cards for a variety of purposes, however due to security concerns, they are only intra domain orientated. The review of the literature demonstrates that efforts have been made globally to tighten the security specifications for smart cards. However, there is no research proposal that claims a single smart card will always be able to handle all application areas. Therefore, a

unique security framework for Internet of Things (IoT) enabled Smart Cards based on Elliptic Curve Cryptography (ECC) is proposed in this research. This is a safe and innovative way for the general population to use one Smart Card to access a variety of smart applications wherever they are. The security assessment confirms that ECC offers robust security for the use of Smart Cards.

Inference: Smart cards are widely used but face security limitations, restricting them to specific domains. This research proposes an innovative security framework using Elliptic Curve Cryptography for IoT-enabled Smart Cards, offering versatile access to various smart applications worldwide while ensuring robust security.

4. **Title:** A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme , Chaturvedi, A., Mishra, D. and Jangirala, S. "A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme, Journal of Information Security and Applications", 2017 , ISSN International Conference. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214212616302897

   Abstract: The Internet of Things (IoT) has revolutionized remote user communication, but it also presents security and privacy challenges. To mitigate these issues, authentication and key agreement (AKA) protocols are being developed. One such protocol is Li et al.'s biometric-based three-factor remote user authentication scheme. However, this scheme is vulnerable to session-specific temporary information attacks and lacks three-factor authentication and user privacy. The authors propose a novel AKA protocol that can overcome these weaknesses without losing its original merits. The proposed scheme is secure against various known attacks, including those found in Li et al.'s scheme. The validity of the proposed scheme is demonstrated using the BAN logic, and it is comparable in terms of computation overheads with Li et al. 's and other related schemes.

   Inference: The IoT has transformed remote communication, but security concerns exist. A biometric-based three-factor authentication protocol by Li et al. has vulnerabilities. Paper proposes a new AKA protocol addressing these issues, ensuring security, privacy, and computational efficiency, comparable to existing schemes.

5. **Title:** Enhancing Security and Privacy in Biometrics-Based Authentication Systems , Ratha, N.K. and Connell, J. "Enhancing security and privacy in biometrics-based Authentication Systems", 2020, ISSN International conference. Available at: https://www.researchgate.net/publication/220353130_Enhancing_Security_and_Privacy_in_Biometrics-Based_Authentication_Systems

   Abstract: Because biometrics-based authentication offers several advantages over other authentication methods, there has been a significant surge in the use of biometrics for user authentication in recent years. It is important that such biometrics-based authentication systems be designed to withstand attacks when employed in security-critical applications, especially in unattended remote applications such as e-commerce. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present new solutions for eliminating some of these weak links. Although, for illustration purposes, fingerprint authentication is used throughout, our analysis extends to other biometrics-based methods.

   Inference: Biometrics-based authentication is growing in popularity, but it must be secure, especially for remote applications like e-commerce. This paper discusses the strengths and weaknesses of biometrics and provides solutions, with a focus on fingerprint authentication but relevance to other biometrics methods.

6. **Title:** Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment , Das, A. and Kumar, N. "Biometrics-based privacy-preserving user authentication Scheme for Cloud-Based Industrial Internet of Things Deployment",2018,IEEE Internet of things Journal. Available at: https://ieeexplore.ieee.org/document/8506419

   Abstract: The Industrial Internet of Things (IIoT) has gained popularity due to the widespread use of Internet-enabled devices. However, security and privacy of shared information remain a concern due to the open channel nature of the Internet. Existing solutions for preserving security and privacy in the IIoT environment are heavy computation and communication overheads. This paper proposes a new biometric-based privacy preserving user authentication (BP2UA) scheme for

cloud-based IIoT deployment. BP2UA consists of strong authentication between users and smart devices using pre-established key agreements. Its formal security analysis using the real-or-random model proves its session key security, while an informal security analysis shows its robustness against known attacks. The computation and communication costs of BP2UA outperform other IoT schemes, and a practical demonstration is conducted using the NS2 simulation.

Inference: The IoT, powered by internet-connected devices, faces security and privacy issues. This paper proposes a biometric-based authentication scheme (BP2UA) for cloud-based IIoT, offering strong security, efficiency, and lower computational and communication costs compared to existing solutions. It is validated through simulation.

7. **Title:** Remote Access Communications Security : Analysis of User Authentication Roles in Organizations , Boateng, E. and Adade, G. "Remote Access Communications Security: Analysis of User Authentication Roles in Organizations",2020,Journal of Information security. Available at: https://www.researchgate.net/publication/342980116_Remote_Access_Communications_Security_Analysis_of_User_Authentication_Roles_in_Organizations

   Abstract: Remote access has become increasingly popular due to the Covid-19 pandemic and the increasing demand for remote work. This has led to increased security concerns for organizations, particularly in the context of remote connectivity technology. The security of corporate cyber assets is at risk due to vulnerabilities in remote users and devices. To address this, an experiment was conducted to analyze user authentication roles. The results showed that 2FA (two-factor authentication) was an effective method for improving remote access security. This involves using the user's mobile phone or soft-token as a second factor, in addition to their password, to overcome security weaknesses inherent in single-factor authentication. However, the study also revealed that remote devices could exhibit further vulnerabilities and pose serious risks to the organization. Therefore, it is crucial to understand how users and remote devices are authenticated and secured to ensure the confidentiality, integrity, and availability of these cyber assets.

Inference: The surge in remote work due to COVID-19 raises security concerns. Two-factor authentication (2FA) is effective for enhancing remote access security, but vulnerabilities in remote devices persist. Ensuring secure user and device authentication is crucial for safeguarding cyber assets.

8. **Title:** Perception and Satisfaction Level of Remote Login Access Users, Jayalakshmi, Rao, M. and K, S.B. "Perception and satisfaction level of remote login access users", 2018, ISSN International conference. Available at: https://digitalcommons.unl.edu/libphilprac/1783

   Abstract: The library is a knowledge centre where all the resources, regardless of print and e-resources, are made available to the user. The study uses a questionnaire-based survey to survey 187 registered users of the library's remote access service. The study identifies the benefits of remote access and the problems faced by registered users to access subscribed e-resources remotely. The study also highlights the importance of remote login access to e-resources in modern library usage, allowing users to access information wherever they are without wasting time. The study suggests some important points for consideration, such as the need for improved user satisfaction and the potential issues faced by registered users in accessing subscribed e-resources remotely.

   Inference: The study focuses on remote access to library resources. It identifies benefits and problems faced by users accessing e-resources remotely. Emphasizing convenience, it underscores the need to improve user satisfaction and address issues with remote access to subscribed resources.

9. **Title:** Secured Policy based Resource Access and User Authentication in Ubiquitous Computing Environment , Pandikumar, S. and Malathi, S. "Secured policy based resource access and user authentication in Ubiquitous Computing Environment", 2019, International Journal of Innovative Technology and Exploring Engineering. Available at: https://www.semanticscholar.org/paper/Secured-Policy-based-Resource-Access-and-User-in-Pandikumar-Malathi/f79c3d813abd284a162401372c6a472135ac9907

Abstract: Context-aware computing focuses on policy-based resource access and data sharing, which can be challenging for wireless and ad hoc users due to various context factors. Mobile phones play a crucial role in information access, and wireless technologies like GSM-SMS are efficient for accessing shared data worldwide with fewer security issues. The proposed system provides systematic access policy schemes and access mechanisms for remote users, based on context information. Users must satisfy defined context and user level, and the mechanism allows them to request and control access through SMS.

Inference: Context-aware computing adapts resource access based on context but poses challenges for wireless users. This system employs mobile phones and GSM-SMS for secure global data access. It enforces access policies based on user-defined context criteria, enabling access control via SMS.

10. **Title:** Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources , Cruz-Piris, L. *et al.* "Access control mechanism for IOT environments based on modeling communication procedures as resources", 2018, ISSN International conference. Available at: https://www.mdpi.com/1424-8220/18/3/917

Abstract: The Internet of Things (IoT) has revolutionized the way we manage data, but the challenge lies in establishing a secure and user-friendly access control scheme for these services. This paper proposes integrating IoT devices into an access control system designed for web-based services by modeling communication elements as resources. This would enable a unified access control scheme between heterogeneous devices. The authors analyze relevant communication protocols and propose a methodology that models communication actions as resources, which can be protected using access control mechanisms. The proposal was validated by selecting Message Queuing Telemetry Transport (MQTT) as a communication protocol and User-Managed Access (UMA) as an access control scheme. Tests were conducted to ensure the system's correctness and to evaluate the energy consumption overhead when using the proposed solution.

Inference: IoT's data management requires secure access control. This paper proposes integrating IoT devices into web-based access control, unifying control across diverse devices. It models communication actions as resources, safeguarded by access control mechanisms. Validation with MQTT and UMA shows system correctness and energy consumption overhead.

2.2 Patent Search

1. **Patent No. US11301554B2**, granted by USPTO dated 2022-04-12 titled, "Secure tamper resistant smart card" depicts a system and methods for secure data management and transfer for secure data transactions. The inventors claim the system as a secure & tamper resistant smart card configured along with immutable store data. Also, it claims to exchange the data via wireless networks/peer to peer networks securely. The smart cards comprise a dedicated hardware circuit blocks electrically coupled via a bus interconnection, a dedicated hardware circuit blocks configured to authenticate users, verify trust amongst the smart card and external devices, and encrypt sensitive data for secure transmission.

2. **Patent No. US20180247483A1**, published on UPSTO Journal dated 2018-08-30, titled, "Security systems for protecting an asset" presents a security system for protecting assets, which includes password-based security systems that can provide different levels of access responsive to entry of a primary or secondary password. In some versions, user-configurable security rules can provide customized responses to entry of primary or secondary passwords, including feigned or limited access, security alerts, etc. Passwords comprising overt and covert components can be used to provide enhanced security and improved user control over system response. Improved security systems involving transactions between multiple parties are also considered, with options for user-customized security rules including primary and secondary passwords, and reverse challenge and response methods.

2.3 Inference Drawn

The evolution of authentication systems reflects an increasing need for heightened security measures, particularly in sectors heavily reliant on digital infrastructure. Traditional methods like passwords and two-factor authentication (2FA) are no longer adequate to combat sophisticated cyber threats. A three-factor authentication system integrating face recognition, voice recognition, and smart card technology offers a robust solution. Face and voice recognition provide biometric authentication, which is difficult to replicate, enhancing security significantly. Smart card technology adds an additional layer of security, requiring physical possession for access. This multi-factor approach not only ensures the authenticity of the user but also reduces the likelihood of unauthorized access. By combining biometric and token-based authentication, organizations can mitigate risks associated with identity theft, data breaches, and unauthorized access attempts. As cyber threats continue to evolve, the adoption of advanced authentication mechanisms like three-factor authentication becomes imperative to safeguard sensitive information and critical infrastructure effectively.

2.4 Comparison with the Existing System

Existing Two-Factor Authentication System	Our Proposed Three-Factor Authentication System
It uses two factors: password-face/ password-voice/ password-card/ face-voice	It uses three factors: crypto card (NFC Smart Card), face, voice
It is vulnerable to stolen card attack and card tampering	It is secured from from stolen card attack and cannot be tampered with (As our crypto card stores data in an encrypted and hashed form and each card has its unique id, the hash value cannot be reversed to the data and hence, even if the card is stolen the hacker won't be able to access the data. Also, if the hacker tries to overwrite the data in the card, the hash value will change and won't match with the hash value in the database)
No liveness detection	The user has to blink their eyes a certain random number of times to detect if they are actually present
It doesn't use crypto cards	It uses NFC enabled smart cards which are coded using cryptography (crypto cards) which make it highly secure against tamper or other attacks
The user data is stored in plain text	The user data is encrypted and then stored in hashed format
Cost of the existing system is ₹7500 (approx. ₹7500-₹8000)	Cost of the proposed system is ₹4010 (approx. ₹4000-₹5000)

Table 2.1: Comparison with Existing System

Chapter 3: Requirement Gathering for the Proposed System

3.1 Introduction to requirement gathering

Requirement gathering is a critical phase in the software development lifecycle, encompassing the systematic gathering and documentation of stakeholders' needs, expectations, and constraints for a software project. This process involves engaging with various stakeholders, including clients, end-users, subject matter experts, and other relevant parties, to understand the purpose, scope, and objectives of the project. Techniques such as interviews, surveys, workshops, and observations are commonly employed to elicit requirements effectively. Additionally, documentation plays a vital role in capturing and organizing gathered requirements, ensuring clarity, traceability, and alignment with project goals. Successful requirement gathering lays the foundation for developing software solutions that meet stakeholders' needs, mitigate risks, and deliver value to the intended users.

3.2 Functional Requirements

- **User Registration:**
    - The system should allow administrators to register authorized users by assigning them unique crypto cards.
    - Users' personal information, such as name, ID, and biometric data, should be collected during registration.
- **Access Control:**
    - Users must be able to present their crypto cards to access sensitive areas.
    - The system should support multiple authentication methods, including face and voice recognition, in addition to the crypto card.
    - Access control decisions should be made in real-time and logged for auditing purposes.
- **Authentication:**
    - The system should verify the authenticity of the crypto card and the user's biometric data before granting access.

    - It should use cryptographic techniques to ensure the integrity of data exchanged during the authentication process.
- **Remote Access:**
    - The system should support remote access to sensitive areas, allowing authorized users to request access from a distance.
    - Secure communication channels should be established for remote access requests.
- **Administrator Dashboard:**
    - Administrators should have access to a dashboard to manage user registrations, revoke access, and monitor access logs.
    - The dashboard should provide real-time alerts for suspicious activities or unauthorized access attempts.
- **Revocation:**
    - The system should support the revocation of crypto cards and access privileges in case of lost cards, personnel changes, or security concerns.
- **Reporting and Logging:**
    - Comprehensive logs of access events, including date, time, user, and access location, should be maintained for auditing purposes.
    - Reporting capabilities should be available for generating access control reports.

3.3 Non-Functional Requirements

- **Security:**
    - The system must adhere to industry-standard security practices to prevent unauthorized access, data breaches, and tampering.
    - Encryption and secure protocols should be used to protect data in transit and at rest.
- **Performance:**
    - The system should provide quick and responsive access control, ensuring minimal delays in granting or denying access.
    - It should handle a high number of concurrent access requests efficiently.

- **Reliability:**
  - The system should have high availability to ensure continuous access control operations, even in the event of hardware or software failures.
  - Backup and redundancy mechanisms should be in place.
- **Scalability:**
  - The system should be able to scale to accommodate an increasing number of users and access points without a significant decrease in performance.
- **Compliance:**
  - The system should comply with relevant data protection and privacy regulations, such as GDPR or HIPAA, depending on the application context.
- **Usability:**
  - User interfaces, both for administrators and users, should be intuitive and user-friendly.
  - Proper training and documentation should be available for users and administrators.
- **Integration:**
  - The system should be compatible with existing access control infrastructure, including door locks, security cameras, and alarm systems.
- **Maintenance:**
  - Regular maintenance and updates should be performed to address security vulnerabilities and system improvements.
  - System downtime for maintenance should be minimized.
- **Cost-Effectiveness:**
  - The system should be designed and implemented in a cost-effective manner, considering both initial setup costs and ongoing operational expenses.

3.4 Hardware, Software, Tools and Techniques utilised

Hardware:

- **Smart Card - MiFare 4K NFC enabled smart card:**
  - MiFare 4K is a type of contactless smart card technology developed by NXP Semiconductors. It operates at 13.56 MHz and is commonly used for various applications such as access control, public transportation, and electronic payment systems.

- The 4K designation indicates the memory capacity of the card, which is 4 kilobytes.

- **Smart Card Reader - ACR122U NFC card reader/writer:**
  - The ACR122U is a USB-based NFC card reader/writer manufactured by Advanced Card Systems Ltd. (ACS).
  - It supports various NFC-based smart cards, including MiFare 4K Classic cards.
  - The ACR122U is compatible with various operating systems including Windows, Linux, and macOS.
  - It's commonly used for tasks such as reading data from smart cards, writing data to smart cards, and interacting with NFC-enabled devices.

Software:

- **Operating System:**
  - Windows 10 or higher: A widely used operating system developed by Microsoft.
  - Ubuntu 20.04: A popular Linux distribution known for its stability and user-friendly interface
- **Python 3.8:**
  - Python is a high-level programming language known for its simplicity and readability.
  - Version 3.8 is one of the stable releases of Python, providing various improvements and new features over previous versions.
- **Python libraries:**
  - numpy==1.23.5: NumPy is a fundamental package for scientific computing with Python, providing support for large, multi-dimensional arrays and matrices.
  - tensorboardX==2.5.1: TensorBoardX is a library for visualization of TensorFlow programs.
  - opencv-python==4.6.0.66: OpenCV (Open Source Computer Vision Library) is a library of programming functions mainly aimed at real-time computer vision.
  - librosa==0.10.1: Librosa is a Python package for music and audio analysis.

- sounddevice==0.4.6: SoundDevice provides Python bindings for PortAudio, the cross-platform audio I/O library.
- soundfile==0.12.1: SoundFile is a Python library to read and write sound files.
- cvzone==1.6.1: CVZone is a Python library built on top of OpenCV for computer vision tasks.
- pyscard==2.0.7: PySCard is a Python module adding smart card support to Python.
- pyusb==1.2.1: PyUSB is a Python module to access USB devices.

Tools:

- **PyCharm IDE 2023.2.5:**
  - PyCharm is an integrated development environment (IDE) used for programming in Python.
  - Version 2023.2.5 is a specific release of PyCharm, offering features such as code completion, syntax highlighting, and debugging tools tailored for Python development.
- **NFC-Tools 6.5:**
  - NFC-Tools is a set of tools for Near Field Communication (NFC) hardware.
  - Version 6.5 is a specific release of NFC-Tools, providing utilities for working with NFC devices and smart cards.
- **Git/GitHub:**
  - Git is a distributed version control system used for tracking changes in source code during software development.
  - GitHub is a web-based platform for hosting and collaborating on Git repositories.

Techniques utilized till date for the proposed system

- **Smart Card Technology:** The system leverages smart card technology as secure tokens to store and transmit unique credentials for authorized users, enhancing physical security.
- **Cryptography:** RSA encryption, a robust cryptographic technique, is utilized to ensure data confidentiality, integrity, and secure communication during the access control process.

- **Biometric Recognition:** The system incorporates face and voice recognition as additional authentication methods, increasing the accuracy of user identification and reducing the risk of unauthorized access.
- **Access Control Algorithms:** Access control algorithms have been implemented to make real-time access control decisions based on the information provided by smart cards and biometric data.
- **User Registration:** The system supports user registration, allowing administrators to assign crypto cards and collect user information for authorization purposes.

3.5 Constraints

To access the system, users must maintain a minimum distance and carry an authentication card. Voice input is required in English only. The system is solely focused on granting access, ensuring security and efficiency. By adhering to these protocols, users can seamlessly interact with the system while maintaining the necessary security measures. Whether it's accessing sensitive information or utilizing system resources, users can trust in the system's dedication to authentication and access control.

Chapter 4: Proposed Design

4.1 Block Diagram of the System

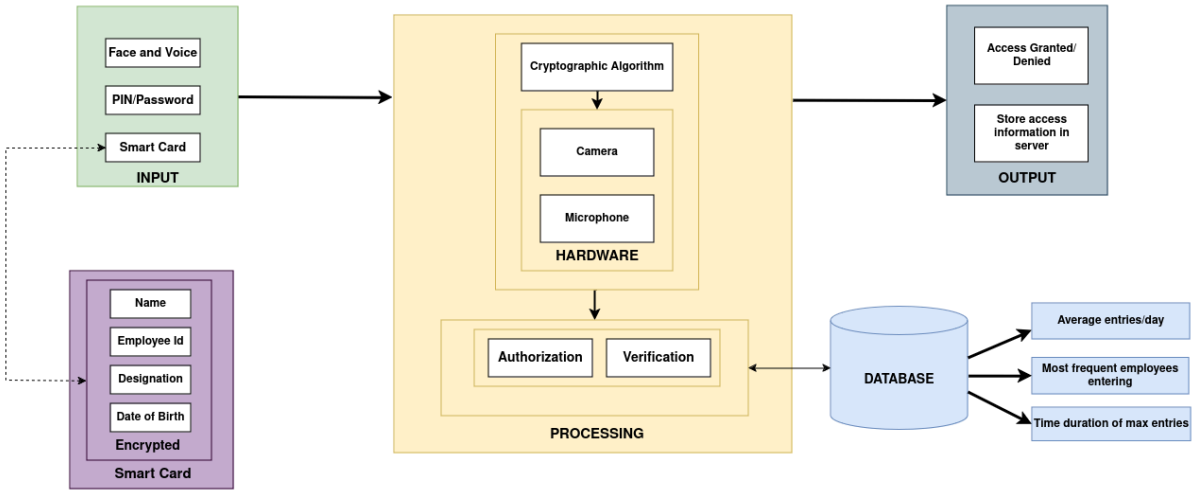

Figure 4.1: Block Diagram

The image represents the block diagram of a Remote Access Control to Sensitive Areas using Crypto Card. Here's a breakdown of the labelled components:

- **Input:** This section refers to the data entering the system from a user. It includes:
  - **PIN/Password:** This refers to a Personal Identification Number that a user would input.
  - **Employee Id:** This refers to the identification number of an employee.
  - **Name:** This refers to the name of the user.
  - **Date of Birth:** This refers to the user's date of birth.
- **Smart Card:** This block represents the smart card itself. It stores the user's identification information and communicates with the reader to facilitate access control.
- **Processing:** This block represents the processing unit that evaluates the user input and determines if access should be granted. It includes:
  - **Camera:** This block represents a camera that is used to capture an image of the user for face recognition and authentication.
  - **Microphone:** This block represents a microphone that is used for voice recognition.

- **Authorization:** This block refers to the process of verifying a user's access rights against the information stored in the database.
- **Verification:** This block refers to the process of verifying the user's identity, such as comparing a PIN entered by the user to the PIN stored on the card or in the database and performing facial and voice recognition using the camera and microphone respectively.

- **Database:** This block represents a database that stores information about authorized users, such as employee IDs, names, access permissions, and their biometric data that includes face data and voice recordings.
- **Output:** This section refers to the data leaving the system:
  - **Access Granted/Denied:** This indicates whether the user has been authorized access to the system or not.
  - **Store access information in server:** This suggests that the system records access attempts in a database, including timestamps and user identification information.

Overall, the block diagram illustrates how a 3 factor authentication system can be used to control access to sensitive areas that need high security. The system authenticates users based on a combination of factors such as PINs and pre-loaded user data on the card that comprises face and voice data of the user.

4.2 Modular design of the system

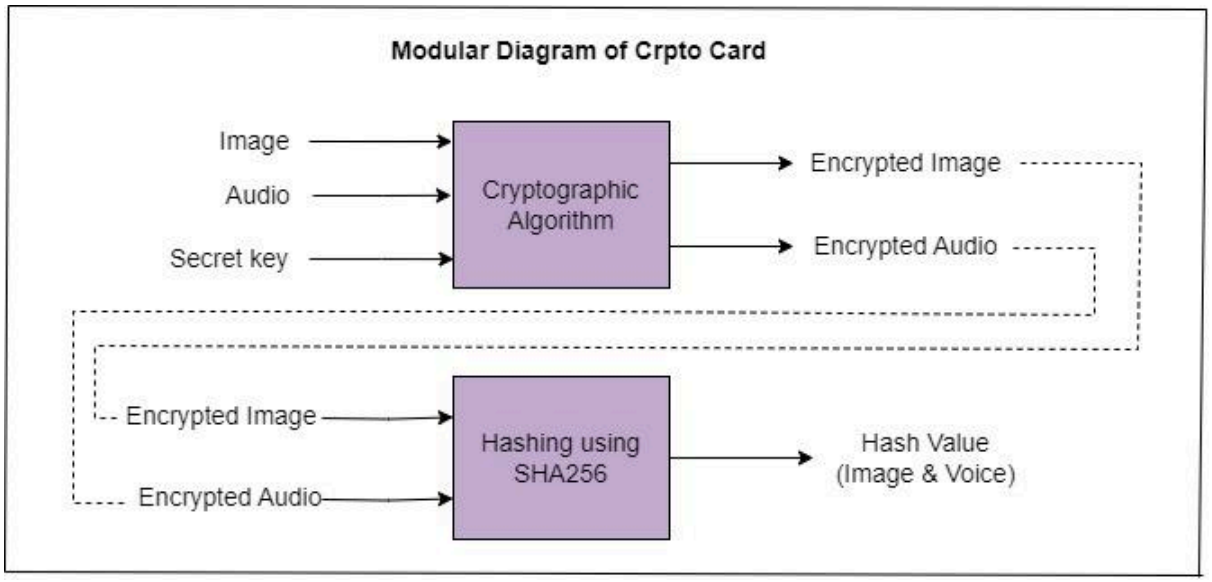

Figure 4.2: Modular Diagram of Smart Card Module

The image represents the modular diagram of a smart card module. The module is responsible for encrypting and decrypting data, specifically images and audio. Here's a breakdown of the labelled components:

- **Image:** This block represents the image data i.e. the face data of the user that is input into the system.
- **Audio:** This block represents the audio data i.e. the voice data of the user that is input into the system.
- **Secret Key:** This block represents the secret key that is used to encrypt and decrypt the data.
- **Cryptographic Algorithm:** This block represents the cryptographic algorithm that is used to encrypt and decrypt the data. The algorithm used is AES (Advanced Encryption Standard) algorithm for encryption and decryption of data.
- **Encrypted Image:** This block represents the encrypted image data.
- **Encrypted Audio:** This block represents the encrypted audio data.
- **Hashing using SHA256 (Image & Voice):** This block refers to the process of generating a hash value of the combined image and audio data using the SHA-256 hashing algorithm.
- **Hash Value:** This block represents the hash value that is generated from the image and audio data.

Overall, the modular diagram illustrates how a smart card module can be used to encrypt image and audio data using a cryptographic algorithm and a secret key. It also shows how a hash value can be generated from the data using a hashing algorithm.

4.3 Detailed Design

a. Data Flow Diagram

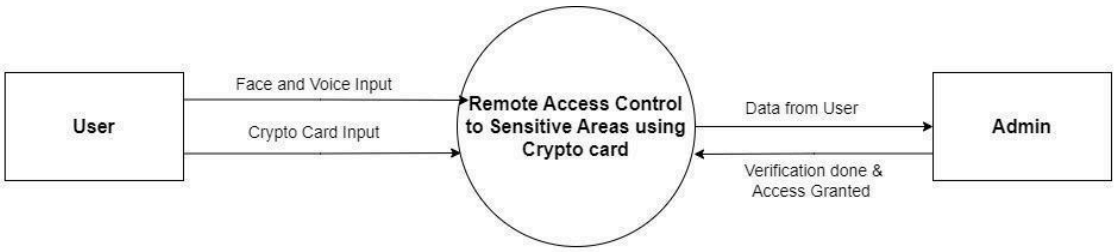

Figure 4.3: Level 0 DFD

The diagram is a Level 0 Data Flow Diagram (DFD) of a Secured Access Control System, illustrating the data flow between the system and its external entities, the User and the Admin. The system has two main processes: verification done & access granted, and remote access control to sensitive areas using a crypto card. The user provides data through Face and Voice input and Crypto Card Input, and the system verifies the user's identity and credentials. If successful, the system grants access to sensitive areas. The Admin receives data like user access logs and security alerts, which they use to monitor and manage the system.

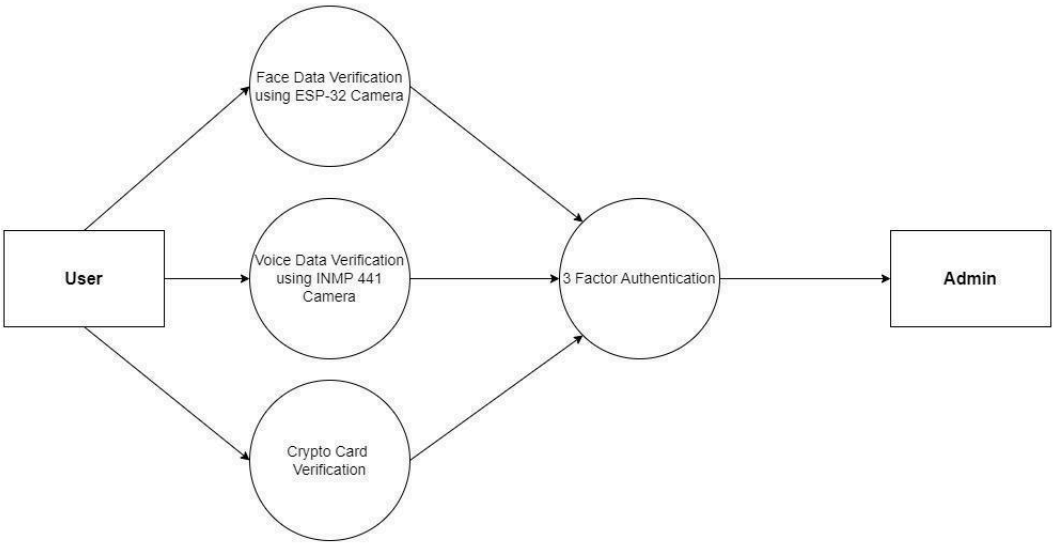

Figure 4.4: Level 1 DFD

The diagram is a Level 1 Data Flow Diagram (DFD) of a Face Data Verification process, illustrating the data flow between the system and its external entities, the User and the Admin. The system has two main processes: Face Data Verification, which verifies the user's identity by comparing their live face data to a stored facial image, and Access Granted / Denied, which grants or denies access based on the outcome of the verification. The system provides data to the Admin, such as user access logs and security alerts, which can be used to monitor and manage the system and detect security threats. The diagram does not detail internal details of the system, such as how the user's face data is compared to the stored facial image or access is granted or denied. It also does not show the data storage component, such as a local database or cloud storage service, nor the security measures in place to protect the facial images from unauthorized access.

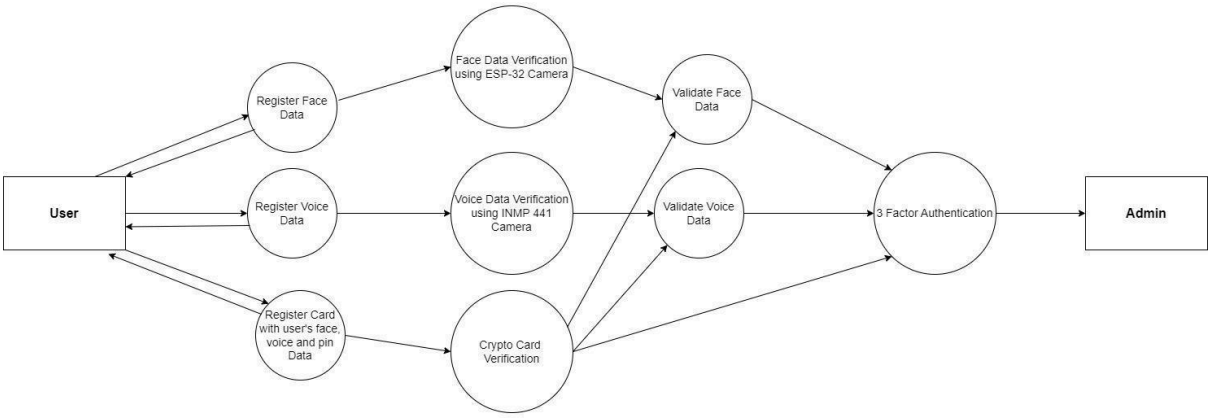

Figure 4.5: Level 2 DFD

The diagram depicts a Level 2 Data Flow Diagram (DFD) of a Face Data Verification process, illustrating the data flow between the system and its external entities, the User and the Admin, as well as internal processes. The system consists of three main processes: Face Data Capture, Preprocessing, and Recognition. The user provides their face data through the ESP-32 Camera, the system preprocesses the data, and performs face recognition on it. If successful, the system grants access to the user, and if not, it denies access. The system also provides data to the Admin, including user access logs and security alerts, which can be used to monitor and manage the system. The diagram also mentions the use of OpenCV library for face detection and recognition, a machine learning model for face recognition, and the data storage component for facial images. The diagram also lacks information on security measures, such as encryption, access control, and intrusion detection.

b. System Design

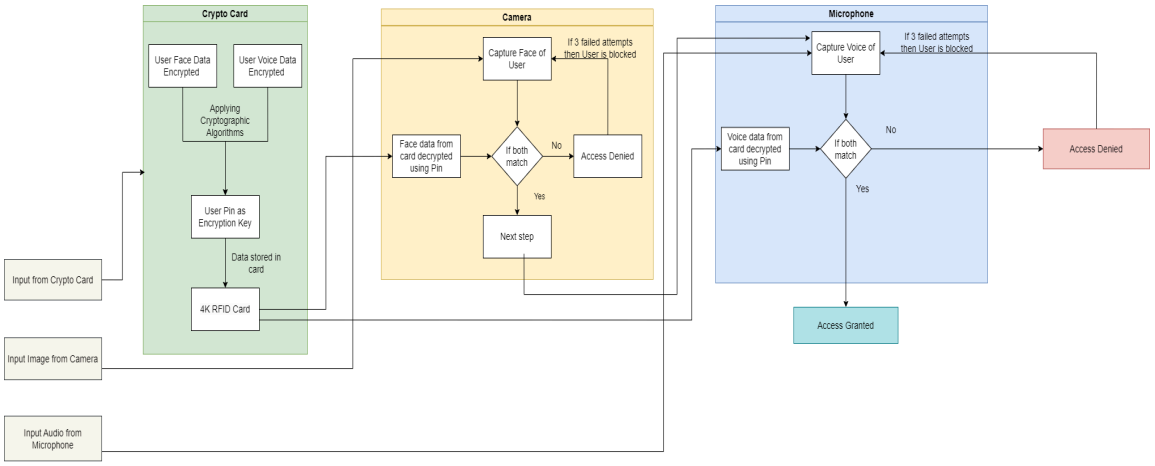

Figure 4.6: System Design

The image represents the system design of our project. There are 3 major factors in our system diagram and they are as follows:

- **Crypto Card:** It consists of the Face and Voice data of a registered user in the system, which is stored in an encrypted and hashed form. The encryption is the secret key the user enters during the registration process. Once the card is read in the system the face and the voice values are decrypted and used further to compare the face and voice of the user.
- **Camera:** The camera unit captures the face of the user, who arrives for face recognition. This unit then compares the face data read from the card and the data that has been captured by the camera. If both the data matches then the user is allowed to proceed for voice authentication, otherwise the user is given 3 attempts, if all these attempts fail then the user is blocked.
- **Microphone:** The microphone unit captures the voice of the user, this unit then matches the captured voice data with the voice data that is already stored. If both match then the user is granted access, otherwise the user is denied access to the system.

c. ER Diagram

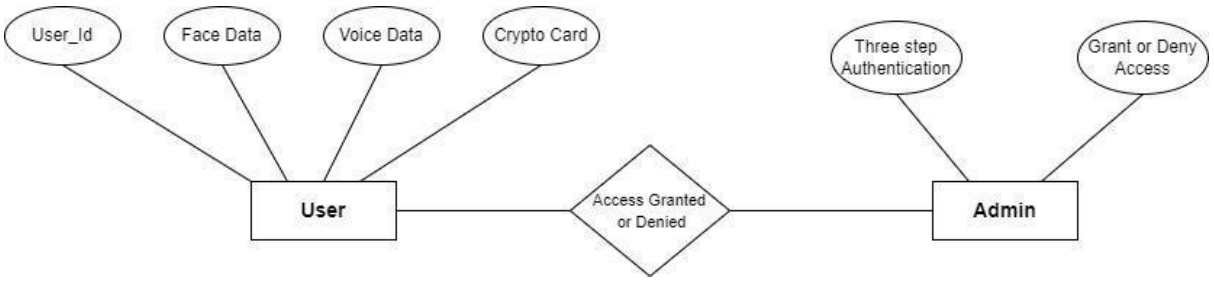

Figure 4.7: ER Diagram

The ER diagram shows the entities and relationships involved in Remote access control verification system using a smart card. The entities are :

- User: A person who uses the remote access control system to access.
- Admin : Admin has the right to grant or deny access to users.

The ER diagram also shows the attributes of each entity. The attributes of the User entity are:

- User ID: A unique identifier for the user.
- Face data : User's facial data (image).

- Voice data : User's voice (audio recording).
- Crypto card : Card in which users' data after encryption is stored as a hash value.

The attributes of Admin entity are :

- 3FA : Admin can check whether the user passes the 3FA or not.
- Grant / Deny access : If admin finds that user passes the 3FA , then it can grant access to user otherwise user will be denied the access.

4.4 Project Scheduling & Tracking using Gantt Chart

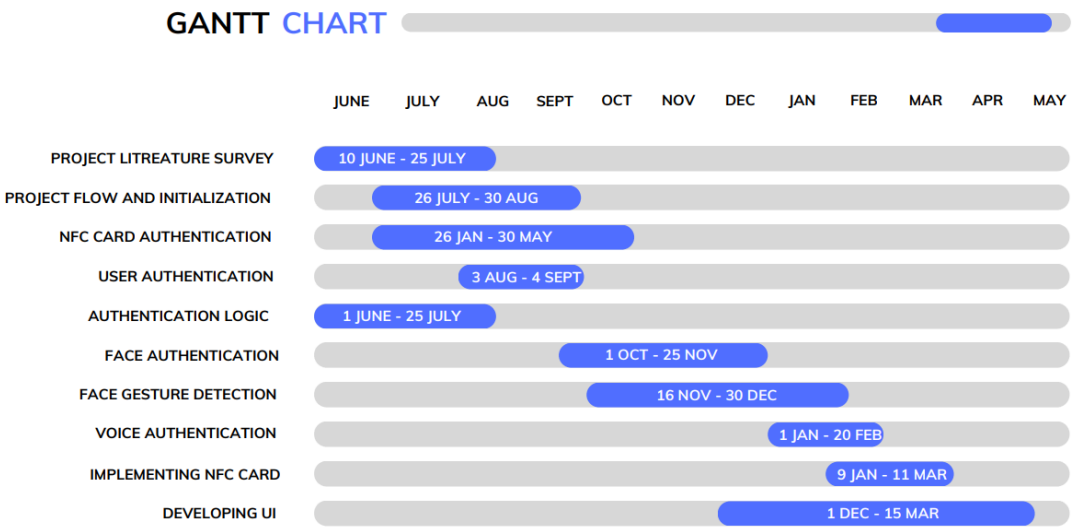

Figure 4.7: Gantt Chart of the system

Chapter 5: Implementation of the Proposed System

5.1. Methodology employed for Development

The proposed methodology for the project focuses on developing a robust and highly secure remote access control system using a three-factor authentication (3FA) approach. This approach integrates smart card technology, encryption techniques, and facial and vocal recognition to create a multi-layered security framework.

- **User Registration:**
  - **Personal Details:** The proposed system starts with the user registration where the users provide their personal information like Name, Employee ID, Date of Birth and a PIN. This PIN is a secret key that is used to encrypt and decrypt the data stored in the NFC Smart Card.
  - **Face Recognition:** Once the user has entered their personal details, they will proceed to register their face data which will capture their unique face points using the face-recognition library and store it in the pickle format in the database.
  - **Voice Recognition:** The users will be prompted to record their voice by saying a unique phrase that will be displayed on the application. The users' voice will be stored in the database in the pickle format.
  - **Data Storage on Smart Card:** After all the data is captured, it will be encrypted first with the PIN that is entered by the user using the AES cryptographic algorithm. The encrypted data will be hashed with SHA-256 and stored on the smart card when the user taps it on the NFC Smart Card Reader ACR122U.
- **User Authentication:**
  - **Smart Card Authentication:** When the user wants to access the system, the first step is smart card verification. The user will have to tap their smart card on the NFC Smart Card Reader and if the hash value stored in the database matches with the one stored on the smart card, they will be prompted for the PIN they created during registration. If the PIN entered by the user is correct, then files storing face and voice data will be decrypted and the user will be allowed to proceed to the next step.

- **Face Authentication:** Once the smart card is verified the next step is face authentication, where the user will have to capture their face in the system's camera and if the face matches with the data stored in the card, the user will be able to move to the next step which is face gesture detection. In this the user will be asked to blink their eyes a random number of times. Once the user blinks the required number of times they will be able to move to the next step.
- **Voice Authentication:** After face authentication the user's voice will be verified. The user will be asked to speak a random phrase that will be displayed on the screen, if the user correctly speaks the phrase and the voice of the user matches with the voice data stored on the card then the user will be granted access to the system.

5.2. Algorithms and Flowcharts for the Respective Modules developed

Algorithms Used:

1. **AES Encryption:** AES is a widely used symmetric encryption algorithm. It operates on fixed-size blocks of data, typically 128 bits. AES uses a secret encryption key for both encryption and decryption. It provides strong data confidentiality and is known for its speed and efficiency. Key lengths of 128, 192, or 256 bits can be used for varying levels of security. Benefits of using AES are:
    - **Symmetric Encryption:** AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. This can simplify key management as you only need to secure the key itself.
    - **High Performance:** AES is known for its speed and efficiency. It can quickly encrypt and decrypt data, making it suitable for real-time applications like remote access control.
    - **Strong Security:** AES is considered highly secure when using an appropriate key length (e.g., 128, 192, or 256 bits). It provides strong data confidentiality, protecting sensitive information from unauthorised access.
    - **Resource Efficiency:** AES encryption and decryption require less computational power compared to some asymmetric encryption algorithms, which can be advantageous in resource-constrained environments.

2. **MD5 Hashing:** MD5 is a cryptographic hash function. It takes variable-length input and produces a fixed-size 128-bit hash value. MD5 is primarily used for data integrity verification, ensuring data hasn't been tampered with. Benefits of using MD5 are:
    - **Data Integrity:** MD5 is a cryptographic hash function that can be used to verify the integrity of data. By comparing the hash of transmitted data with the original hash, you can detect any changes or tampering.
    - **Speed:** MD5 is a fast-hashing algorithm, making it suitable for quickly generating hash values for data verification.

Flowcharts:

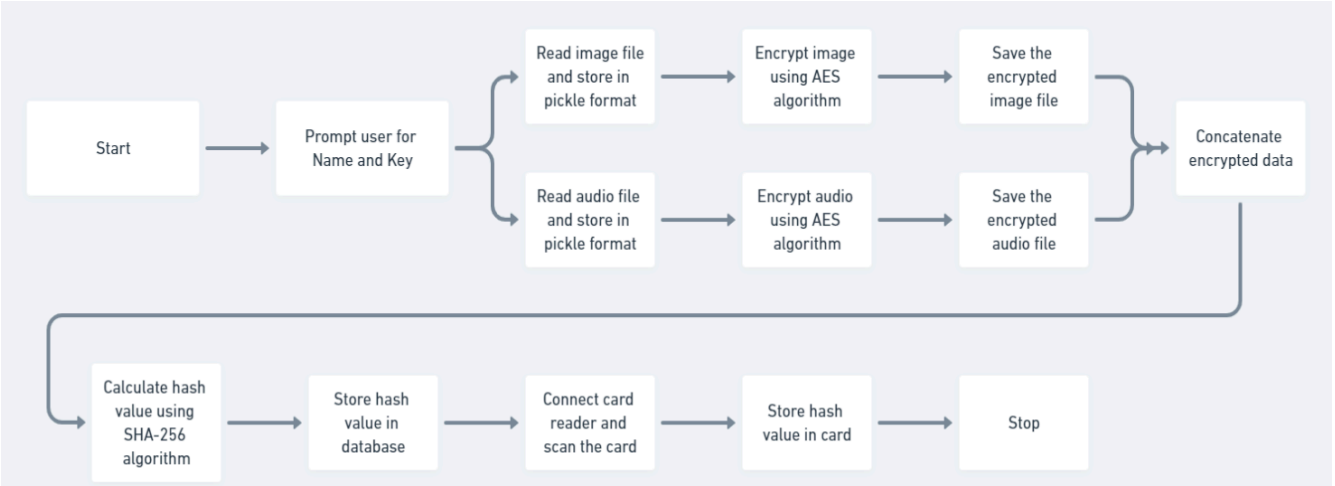

Figure 5.1: Flowchart of Steps for Registration of User

The image depicts the flowchart of our project's registration process. Here's a breakdown of the flowchart:

1. **Start:** The process begins here.
2. **Prompt user for Name and Key:** The user is prompted to enter their personal details like name, key, etc. Here the name is the name of the user registering in the system and the key is the secret key which will be used for encryption and decryption.
3. **Read image file:** The image file containing the user's face and voice data that will be encrypted is read.
4. **Encrypt image using AES algorithm:** The image file is encrypted using the Advanced Encryption Standard (AES) algorithm. AES is a symmetric block cipher that can be used to encrypt and decrypt information.

5. **Encrypt audio using AES algorithm:** The audio file is encrypted using the AES algorithm.
6. **Save the encrypted image & audio file:** The encrypted image and audio file is saved. The file format used is pickle, a file format used in Python for serializing and de-serializing object structures.
7. **Calculate hash value using SHA-256 algorithm:** A hash value is calculated for the encrypted image and audio files using the SHA-256 hashing algorithm. SHA-256 is a cryptographic hash function that generates a unique fixed-size string of bits as its output.
8. **Store hash value in database:** The hash value is stored in a database.
9. **Connect card reader and scan the card:** A card reader is connected, and a card is scanned. The purpose of this step is not entirely clear from the flowchart.
10. **Store hash value in card:** The hash value is stored on the card.
11. **Stop:** The process ends here.

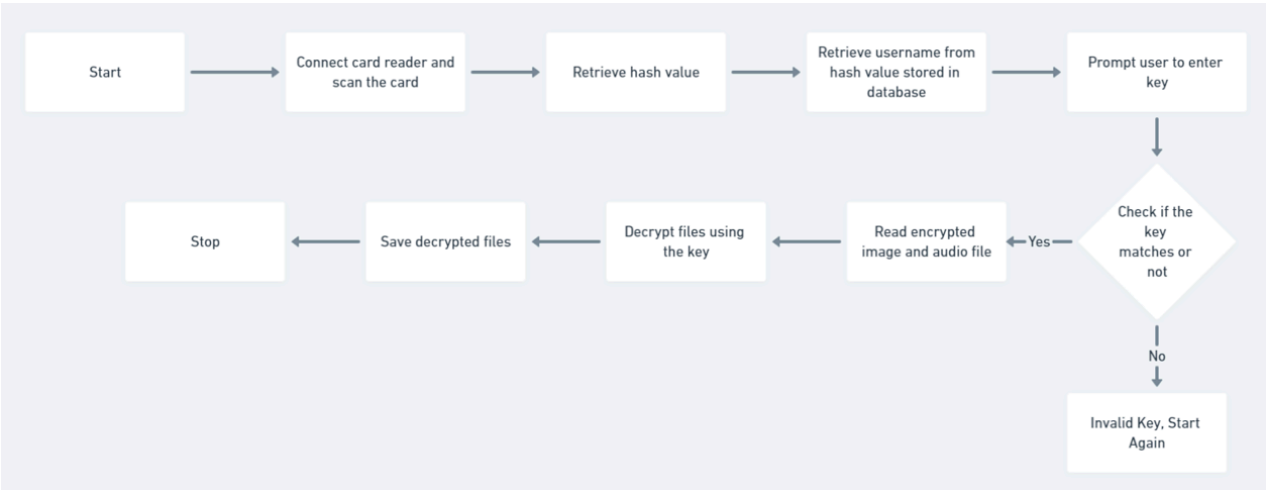

Figure 5.2: Flowchart of Steps for Authentication of User

The image depicts the flowchart of our project's authentication process. Here's a breakdown of the flowchart:

1. **Start**: The process begins here.
2. **Connect card reader and scan the card**: A card reader is connected to the system and the user's card is scanned. This action retrieves a hash value.
3. **Retrieve hash value from database**: The hash value stored in the database is retrieved.

4. **Compare hash value of card and database**: The hash value extracted from the card is compared with the hash values stored in the database. If a match is found then the name of the user is extracted otherwise the user does not exist is displayed.
5. **Prompt user to enter key**: The user is prompted to enter the secret key value which the user sets during the registration process.
6. **Check if key matches or not**: The system checks if the key entered by the user matches the hash value retrieved from the card.
7. **Yes**: If the key matches the hash value, the process proceeds to step 8.
8. **Read encrypted image and audio file**: The encrypted image and audio file are read.
9. **Decrypt files using the key**: The encrypted files are decrypted using the key.
10. **Save decrypted files**: The decrypted files are saved.
11. **No**: If the key entered by the user does not match the hash value, the process proceeds to step 12.
12. **Invalid Key, Start Again**: The user is informed that the key is invalid and the process returns to the beginning at step 1.

Chapter 6: Testing of the Proposed System

6.1 . Introduction to Testing

For the testing phase of the remote access control system, various aspects of functionality were thoroughly examined. This included testing the system's ability to detect spoofing attempts, voice duplication, stolen card attack and ensuring successful authentication under different scenarios.

6.2 Types of Tests Considered

1. **Functional Testing:** This type of testing ensures that each function of the remote access control system works as intended. It involves testing features like user authentication, access control, and logging capabilities.
2. **Security Testing:** Security testing focuses on evaluating the system's ability to resist unauthorized access attempts and protect sensitive data. This includes testing for vulnerabilities such as spoofing attempts, voice duplication, and stolen card attacks.
3. **Performance Testing:** Performance testing assesses the system's responsiveness and stability under various loads and scenarios. It helps ensure that the system can handle expected user traffic without experiencing significant slowdowns or crashes.
4. **Usability Testing:** Usability testing evaluates the system's user-friendliness and accessibility for end-users. It involves testing user interfaces, navigation flows, and overall user experience to identify areas for improvement.
5. **Compatibility Testing:** Compatibility testing checks the system's compatibility with different devices, operating systems, and web browsers. It ensures that users can access the system seamlessly regardless of their device or platform.
6. **Integration Testing:** Integration testing verifies the seamless integration of different system components and modules. It ensures that all parts of the system work together properly to deliver the intended functionality.

6.3 Various Test Case Scenarios Considered

1. **Personal Details:** The user needs to fill in all the details without which he or she is not being allowed to move on to the next step.
2. **Face Authentication:** The user will be allowed to proceed to the next step if and only if they pass the face authentication phase that is their face matches and they complete the gesture detection process. If the user won't be able to go the next step without validating their face.
3. **Voice Authentication:** The user will have to speak a random phrase in the microphone that will be displayed on the screen. If the user's voice matches and they phrase they are speaking matches then they will be granted access.
4. **Card Attack Prevention:** Every Cryptocard has its unique id and that is stored in the database, so if any other card that is not registered is used to access the system the system will deny that user the access.
5. **Stolen Card Attack Prevention:** If a card is stolen by a hacker they won't be able to access the data in the card or even change the data in the card, as the data stored in the card is first encrypted and then hashed. Hash values are not reversible and hence this provides maximum security.
6. **Successful Authentication Scenarios:** When a user enters a valid cryptocard and then enters the correct key and then their face is authenticated followed by fulfilling the gesture detection and speaking the correct phrase and if their voice matches then the system grants access.
7. **Unsuccessful Authentication Scenarios:**
    - Case 1: Invalid Card

      If the card is not registered in the system then the user will not be granted access to the system.
    - Case 2: Incorrect Pin/Password

      If the user enters Pin/Password while authentication then the system will give the user 2 more chances and if they still enter the wrong pin or password then the system will block the user.
    - Case 3: Face Does not Match

      If the face of the user does not match with the data stored during registration the user will not be able to move to the next step terminating the authentication process there itself.
    - Case 4: Gesture Detection Condition is not satisfied

If the user does blink the number of times that has been mentioned then the system will not let the user proceed to the next step of authentication.

- Case 5: Voice does not match

  If the user's voice does not match with the voice data stored during the registration process then the system will deny access to the user.

- Case 6: Phrase spoken doesn't match

  If the phrase spoken doesn't match the phrase displayed on the screen then the user won't be granted access to the system.

6.4 Inference Drawn from the Test Cases

The testing results demonstrated that the remote access control system effectively detects spoofing attempts, as evidenced by its ability to differentiate between live faces and images. Additionally, authentication was consistently successful for registered users, with over 50 students successfully authenticated without encountering any issues. These findings indicate the system's reliability and effectiveness in providing secure remote access control, bolstering confidence in its ability to safeguard sensitive data and resources. The comprehensive testing approach ensured that various aspects of functionality and security were thoroughly examined, leading to valuable insights into the system's performance and capabilities.

Chapter 7: Results and Discussions

7.1. Screenshots of User Interface (UI) for the Respective Module

Figure 7.1: Landing Page of Registration

The image depicts the landing page for registration of Remote Access Control to Sensitive Areas using Crypto Card.

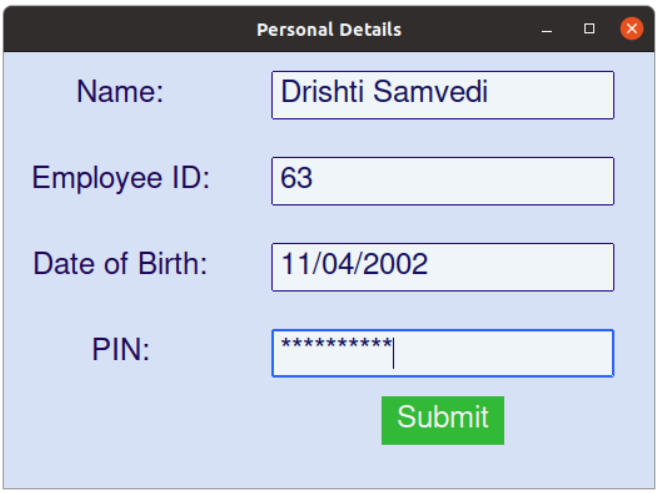

Figure 7.2: Form to enter the personal details

The user has to enter his personal details including Name, Employee Id, Date of Birth and PIN that will be stored on the smart card.

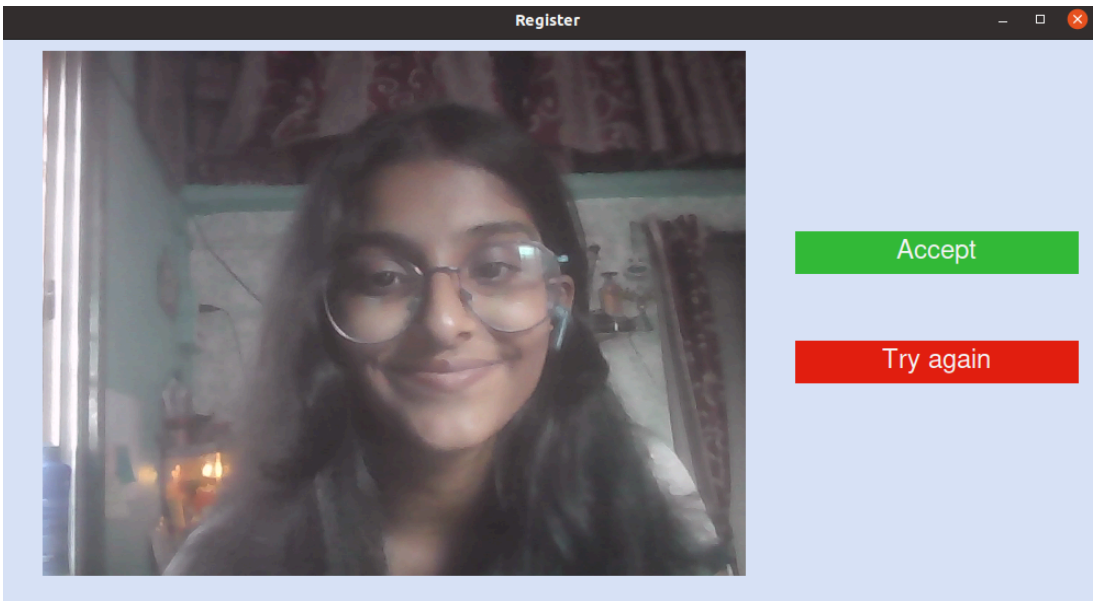

Figure 7.3: Capture your face

The image shows the captured facial data of the user. Users have the option to accept this image for registration or try again to capture a new image.

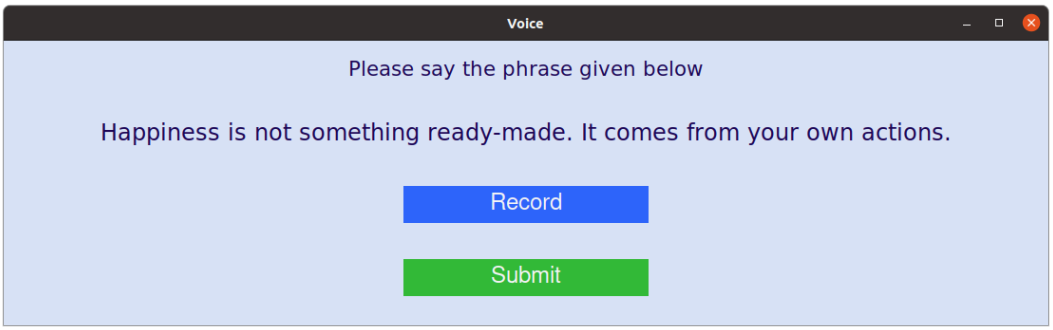

Figure 7.4: Record your voice

The image depicts the phrase that the user has to speak to record their voice. The phrase is generated at random.

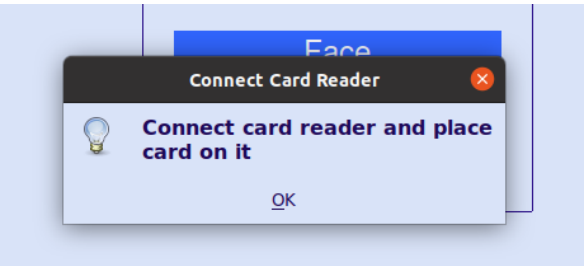

Figure 7.5: Connect NFC Smart Card Reader and place Card on it

The image prompts the user to connect the card reader and tap the smart card on it.

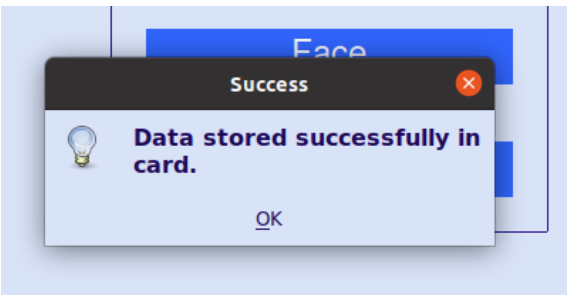

Figure 7.6: Data successfully stored in the card

The image depicts that user data is successfully stored in the smart card.

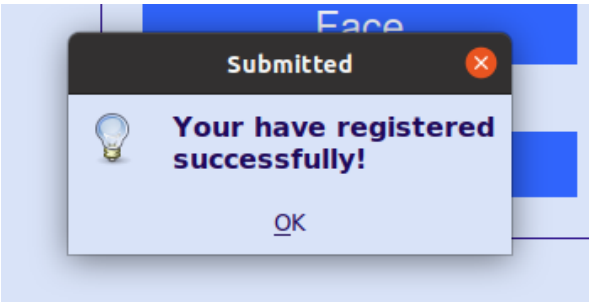

Figure 7.7: Registration Successful

The image depicts that the user has successfully completed the registration process.

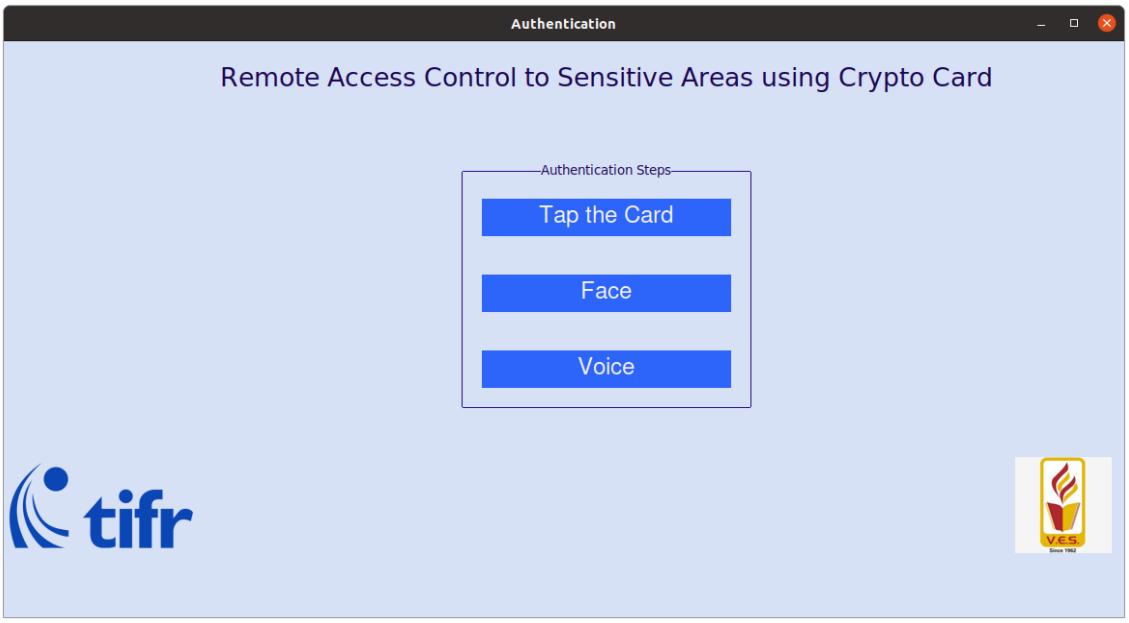

Figure 7.8: Landing Page for Authentication

The image depicts the landing page for authentication of Remote Access Control to Sensitive Areas using Crypto Card.

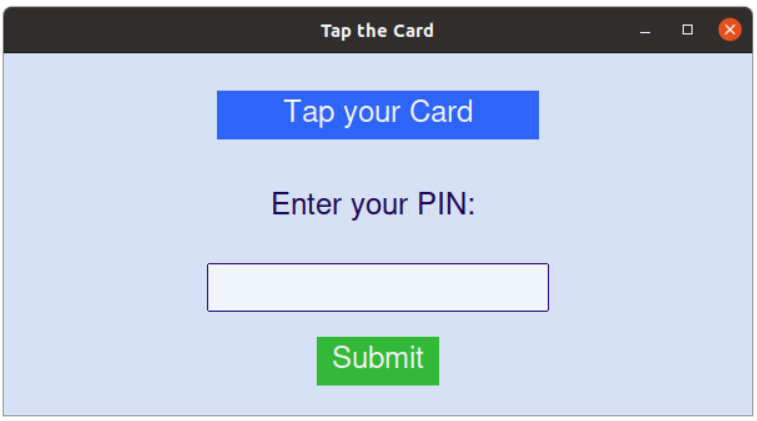

Figure 7.9: Tap your card on NFC Smart Card Reader

The image prompts the user to tap the smart card and then enter the pin.

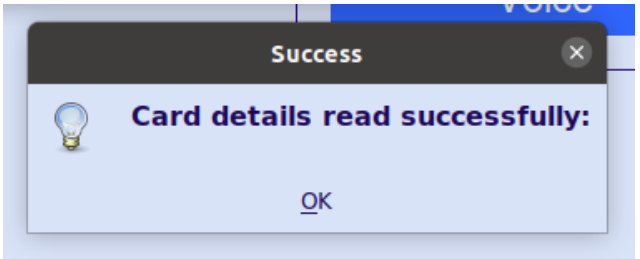

Figure 7.10: Card details successfully read

The image depicts that the card details have been successfully read.

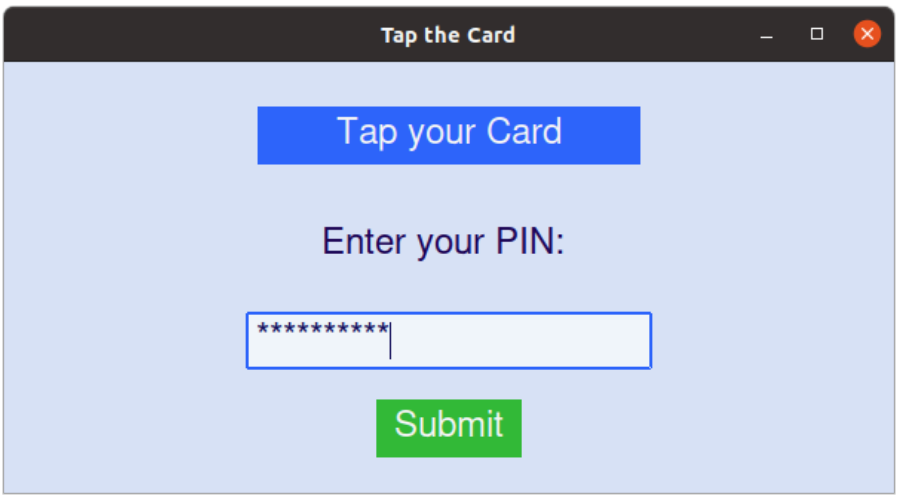

Figure 7.11: Enter PIN after tapping your card

The image shows that the user is prompted to enter the PIN that they used during registration.

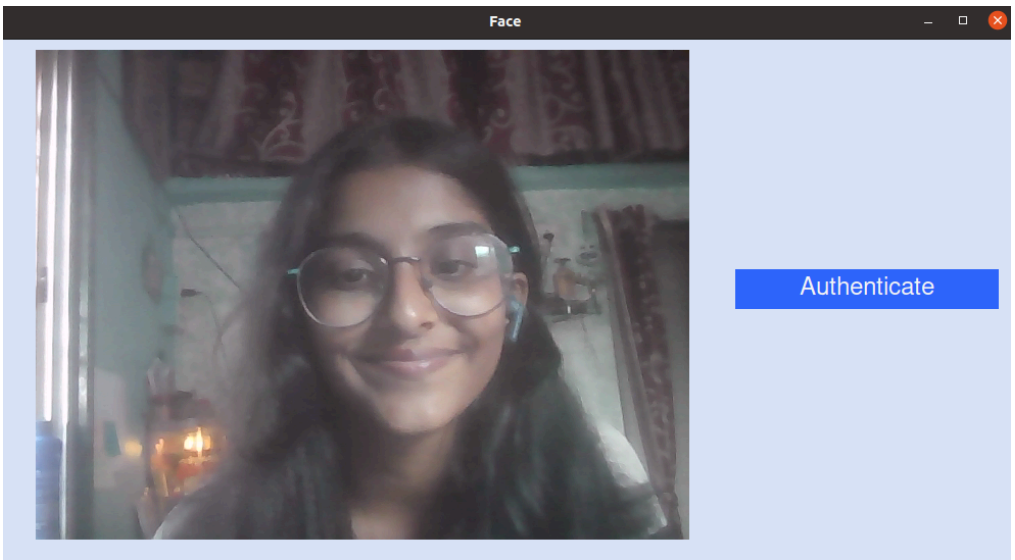

Figure 7.12: Face Authentication

Once the user is done with the smart card authentication, they will proceed for face authentication.

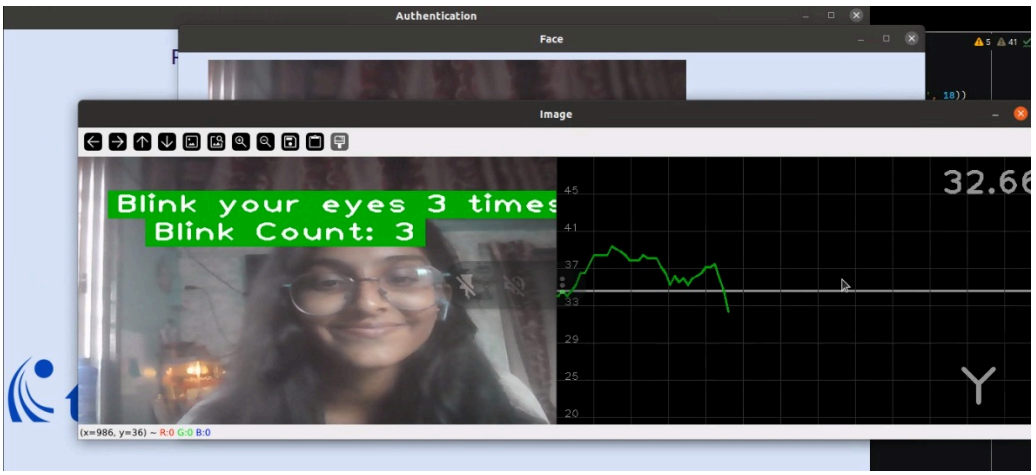

Figure 7.13: Blink eyes for given number of times

The image depicts the result of the eye blink counter, which verifies that the user is present in person while face authentication.

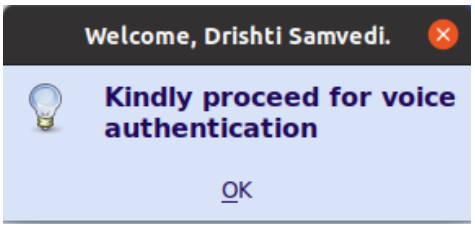

Figure 7.14: After successful face authentication, proceed for voice authentication

The image prompts the user to proceed for voice authentication after the face is authenticated.

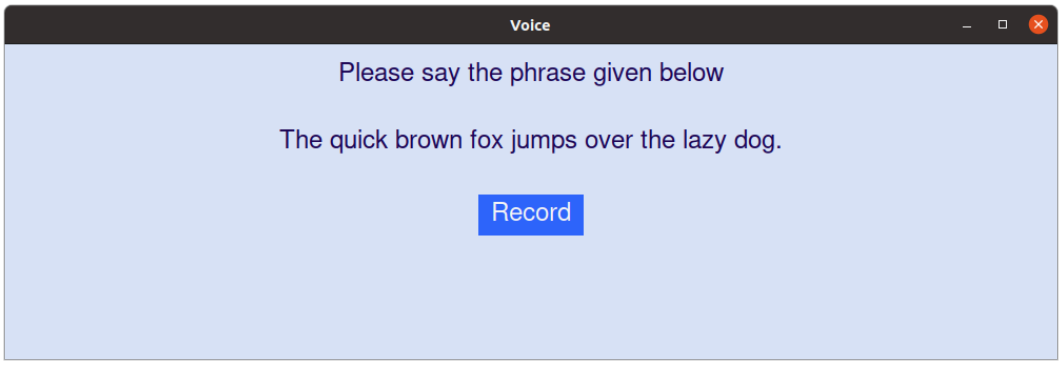

Figure 7.15: Record your voice by saying the given phrase

The image asks the user to record their voice by saying the phrase that is given on the screen.

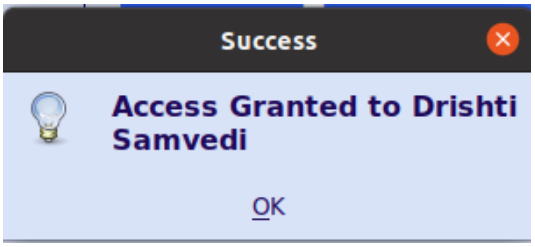

Figure 7.16: Access granted if all factors match

The image depicts that user is successfully authenticated and granted access to the system.

7.2. Performance Evaluation Measures

For the performance evaluation of the remote access control system, several key measures were considered. These measures included response time, throughput, resource utilization, and system scalability. Response time was measured to assess the system's speed in processing user requests, while throughput evaluated the system's ability to handle concurrent requests. Resource utilization metrics such as CPU and memory usage provided insights into the system's efficiency. Additionally, scalability testing was conducted to determine how the system's performance varied with increasing user loads. It is proposed to evaluate our system on the following evaluation measures:

1. **Efficiency:** Efficiency concerns how well the code performs its operations in terms of resource usage and speed. Fernet encryption is relatively efficient and fast for small to medium-sized files. For large files, the performance might be impacted. The project handles errors or exceptions that may occur during file operations, key management, or encryption.

- **Time efficiency** = (Average time taken to encrypt and decrypt an image and audio file of a certain size) / (Total time taken to encrypt and decrypt all image and audio files)
- **Memory efficiency** = (Average amount of memory used by the encryption algorithm) / (Total amount of memory used to encrypt and decrypt all image and audio files)

2. **Accuracy:** The project is primarily focused on encryption and hashing, which should not significantly affect the accuracy of the data. The accuracy of the encryption depends on the strength of the encryption key (Fernet key) and the encryption algorithm (Fernet). Fernet is a symmetric encryption algorithm, and as long as the key is kept secret and secure, the accuracy of the encryption should be reliable
    - **Bit accuracy** = (Number of bits that are not corrupted when encrypting and decrypting all image and audio files) / (Total number of bits in all image and audio files)
    - **Hash accuracy** = (Number of true positives and true negatives when using the hash function to verify the integrity of all image and audio files) / (Total number of positives and negatives when using the hash function to verify the integrity of all image and audio files)
3. **Security:** Security is a critical aspect of the project. The use of Fernet encryption is generally secure when a strong key is used. The custom_key used in the code should be generated and stored securely. In a real-world scenario, you should generate a strong and random key and manage it securely. The hash value (SHA-256) is calculated to verify data integrity, which is a good security practice.
    - **Encryption security** = (Number of image and audio files that cannot be decrypted by an attacker) / (Total number of image and audio files)
    - **System security** = (Number of vulnerabilities in the system that cannot be exploited by an attacker) / (Total number of vulnerabilities in the system)
4. **Sensitivity:** Sensitivity refers to how well the code protects sensitive data. In this case, it encrypts image and audio data, which can be sensitive. The project uses Fernet encryption, which is a strong encryption algorithm, and it's designed to protect data confidentiality.
    - **Data sensitivity** = (Number of image and audio files that cannot be accessed or modified by an attacker) / (Total number of image and audio files)

Overall Evaluation: The project is an efficient, accurate, secure, and sensitive way to implement the remote access control using smart cards. This project is a basic demonstration of encrypting image and audio data using AES encryption and calculating a SHA-256 hash value and storing it in a smart card which can later be used for authentication. It is relatively easy to implement, and it is a good choice for most applications.

7.3. Input Parameters Considered

Various input parameters were considered during performance evaluation, including the number of concurrent users, the frequency of access requests, and the size of data packets transmitted. These parameters were varied to simulate different usage scenarios and evaluate the system's performance under varying conditions.

7.4. Graphical and Statistical Output

Graphical representations and statistical analysis were utilized to present the performance evaluation results. Graphs illustrating response time trends, throughput rates, and resource utilization were generated to visualize the system's performance metrics. Statistical analysis, including mean, median, and standard deviation, provided quantitative insights into the system's performance characteristics.

7.5. Comparison of Results with Existing Systems

The performance evaluation results were compared with those of existing access control systems to assess the efficacy of the remote access control system. Key performance metrics such as response time, throughput, and resource utilization were compared to determine if the system outperformed or was comparable to existing solutions in terms of performance efficiency.

7.6. Inference Drawn

The performance evaluation revealed that the remote access control system demonstrated satisfactory performance across various metrics. Response times were within acceptable limits, throughput rates met expected levels, and resource utilization remained efficient even under high user loads. Comparison with existing systems showed that the remote access control system offered competitive performance, indicating its suitability for deployment in

real-world scenarios. These findings infer that the system's architecture and design are capable of delivering reliable and efficient remote access control services, meeting the performance requirements of modern applications.

Chapter 8: Conclusion

8.1 Limitations

While our system boasts several features and functionalities, it also faces some limitations and constraints. The requirement for good lighting conditions and a single individual in front of the screen during face detection could pose challenges in environments with variable lighting or high foot traffic. Additionally, the constraint mandating a minimum distance from the system might limit its usability in crowded spaces or areas with spatial constraints. The system's reliance on English language input for voice authentication may present difficulties for non-English speakers, impacting inclusivity. Moreover, the necessity for users to carry authentication cards introduces an additional requirement and potential inconvenience for users. Furthermore, the system's sole focus on granting access overlooks the possibility of incorporating features for monitoring attendance discrepancies or providing feedback to users, limiting its utility beyond basic access control. These limitations underscore the importance of considering environmental factors, user diversity, and operational contexts when designing and deploying touchless attendance systems.

8.2 Conclusion

In conclusion, the project to develop a highly secure remote access control system using a three-factor authentication (3FA) approach, combining smart card technology, encryption methods, and facial and vocal recognition, represents a significant stride in enhancing access security and user convenience. By implementing this multi-layered authentication system, we have effectively addressed the vulnerabilities associated with traditional password-based systems. The incorporation of smart cards as the initial factor ensures that only authorized individuals with valid credentials can initiate the authentication process. The subsequent requirement of a PIN or password adds an extra layer of knowledge-based security. The pinnacle of this approach is the use of facial and vocal recognition, harnessing the power of biometrics to validate the user's identity, making it exceedingly difficult for unauthorized entities to gain access. This project not only bolsters security but also caters to the user's comfort, as it eliminates the need for cumbersome password management. It stands as a testament to the ever-evolving landscape of access control, where data protection, user experience, and security converge. In today's world, where digital threats are constantly

evolving, this project represents a vital step towards safeguarding critical assets, data, and the privacy of individuals in sensitive areas.

8.3 Future Scope

To implement multilingual support for voice authentication enhances the inclusivity and usability of the touchless attendance system, allowing users to interact with the system in their preferred language. By incorporating advanced speech recognition algorithms trained on diverse linguistic datasets, the system can accurately authenticate users across various languages, ensuring a seamless user experience. Moreover, the integration of an extra layer for gesture detection, such as finger counting, adds an additional level of security and accessibility. This feature enables users to perform a simple gesture, like counting fingers, alongside voice authentication, further validating their identity and reducing the risk of unauthorized access. Real-life testing and deployment in organizations play a crucial role in validating the system's performance, usability, and security under real-world conditions. Through extensive testing and refinement based on feedback from organizations, the remote access control system can be fine-tuned to meet specific user requirements and operational needs, ensuring its effectiveness and reliability in diverse workplace environments.

References

[1] Patel, C. and Doshi, N., "A novel MQTT security framework in generic IOT model", 2020, ISSN International conference. Available at: https://www.sciencedirect.com/science/article/pii/S1877050920311297

[2] Amin, R. *et al.* "An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography", 2015, Springer. Available at: https://link.springer.com/article/10.1007/s10916-015-0351-y

[3] T. D. Premila Bai, K. M. Raj and S. A. Rabara, "Elliptic Curve Cryptography Based Security Framework for Internet of Things (IoT) Enabled Smart Card", 2017, World Congress on Computing and Communication Technologies (WCCCT). Available at: https://ieeexplore.ieee.org/document/8074489

[4] Chaturvedi, A., Mishra, D. and Jangirala, S. "A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme, Journal of Information Security and Applications", 2017, ISSN International Conference. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214212616302897

[5] Ratha, N.K. and Connell, J. "Enhancing security and privacy in biometrics-based Authentication Systems", 2020, ISSN International conference. Available at: https://www.researchgate.net/publication/220353130_Enhancing_Security_and_Privacy_in_Biometrics-Based_Authentication_Systems

[6] Das, A. and Kumar, N. "Biometrics-based privacy-preserving user authentication Scheme for Cloud-Based Industrial Internet of Things Deployment", 2018, IEEE Internet of things Journal. Available at: https://ieeexplore.ieee.org/document/8506419

[7] Boateng, E. and Adade, G. "Remote Access Communications Security: Analysis of User Authentication Roles in Organizations", 2020, Journal of Information security. Available at:https://www.researchgate.net/publication/342980116_Remote_Access_Communications_Security_Analysis_of_User_Authentication_Roles_in_Organizations

[8] Jayalakshmi, Rao, M. and K, S.B. "Perception and satisfaction level of remote login access users", 2018, ISSN International conference. Available at: https://digitalcommons.unl.edu/libphilprac/1783

[9] Pandikumar, S. and Malathi, S. "Secured policy based resource access and user authentication in Ubiquitous Computing Environment", 2019, International Journal of Innovative Technology and Exploring Engineering. Available at: https://www.semanticscholar.org/paper/Secured-Policy-based-Resource-Access-and-User-in-Pandikumar-Malathi/f79c3d813abd284a162401372c6a472135ac9907

[10] Cruz-Piris, L. *et al.* "Access control mechanism for IOT environments based on modelling communication procedures as resources", 2018, ISSN International conference. Available at: https://www.mdpi.com/1424-8220/18/3/917

Appendix

a. Patent published

4/5/24, 8:39 AM Intellectual Property India

Office of the Controller General of Patents, Designs & Trade Marks
Department for Promotion of Industry and Internal Trade
Ministry of Commerce & Industry,
Government of India

(http://ipindia.nic.in/index.htm)

INTELLECTUAL PROPERTY INDIA (http://ipindia.nic.in/index.htm)

Application Details	
APPLICATION NUMBER	202421017990
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	13/03/2024
APPLICANT NAME	**1 . Dr. Gresha S Bhatia** **2 . Mrs. Abha Tewari** **3 . Dr. Shashikant Raichand Dugad** **4 . Mr. Om Mahadev Madat** **5 . Mr. Figo Evander Cardozo** **6 . Mr. Vansh Rajesh Pahuja** **7 . Ms. Drishti Prakash Samvedi**
TITLE OF INVENTION	A SYSTEM AND A METHOD FOR REMOTE ACCESS CONTROL TO SENSITIVE AREAS USING CRYPTO CARD
FIELD OF INVENTION	COMPUTER SCIENCE
E-MAIL (As Per Record)	abha.tewari@ves.ac.in
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	13/03/2024
PUBLICATION DATE (U/S 11A)	05/04/2024

Application Status

4/5/24, 8:39 AM Intellectual Property India

APPLICATION STATUS	**Application Awaiting Examination**

View Documents

Filed → RQ Filed → Published → Under Examination → Disposed

In case of any discrepancy in status, kindly contact ipo-helpdesk@nic.in

b. Project review sheet

Inhouse/ Industry_Innovation/Research: (TIFR).

Sustainable Goal:

Project Evaluation Sheet 2023 - 24

Class: D17 A/B/C

Group No.: 5

Title of Project: Remote Access Control to Sensitive Areas Using Crypto Card.

Group Members: Figo Cardozo (D17A/08), Om Madat (D17A/38), Vansh Pahuja (D17A/50), Drishti Samvedi (D17B/63)

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
05	05	04	03	04	02	02	02	02	02	03	03	03	03	05	48

Comments: Highlight your proposed sys as compared to existing systems, Constraints, sys design update, Evaluation measures, Integration, dashboards.

Dr. G Bhatia

Name & Signature Reviewer1

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
05	05	04	03	04	02	02	02	02	02	03	03	03	03	05	48

Comments:

Date: 10th february, 2024

Priyanka

Name & Signature Reviewer 2

Inhouse/ Industry_Innovation/Research:

Sustainable Goal:

Project Evaluation Sheet 2023 - 24

Class: D17 A/B/C

Group No.: 5

Title of Project: Remote Access Control to Sensitive Areas Using Crypto Card.

Group Members: Figo Cardozo (D17A/08), Om Madat (D17A,38), Vansh Pahuja (D17A,50), Drishti Samvedi (D17B,63)

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
5	5	5	3	5	2	1	2	2	2	3	2	3	3	5	48

Comments: Future Scope, Advantages, Disadvantages, Constraints, UI & dashboard for login time of employee.

Dr. Geetha Bhatia 9/3/24

Name & Signature Reviewer1

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
05	05	05	03	05	02	01	02	02	02	03	02	03	03	05	48

Comments:

Date: 9th March, 2024

Priyanka Swagde

Name & Signature Reviewer 2

c. Competition Certificates

Vivekanand Education Society's Institute Of Technology, Mumbai

An Autonomous Institute affiliated to University of Mumbai, approved by AICTE

In association with VESIT - IQAC & VESIT - IIC

Department Of Computer Engineering

CERTIFICATE OF EXCELLENCE

This to certify that Figo Cardozo of D17A has won 3rd prize at Department Technology Day, **Pradarshini '24** conducted on 22nd-23rd March 2024.

DR. MRS. NUPUR GIRI
HOD, COMPUTER DEPARTMENT

DR. MRS. GRESHA BHATIA
DHOD, COMPUTER DEPARTMENT

PROJECT COORDINATOR
COMPUTER DEPARTMENT

Vivekanand Education Society's Institute Of Technology, Mumbai

An Autonomous Institute affiliated to University of Mumbai, approved by AICTE

In association with VESIT - IQAC & VESIT - IIC

Department Of Computer Engineering

CERTIFICATE OF EXCELLENCE

This to certify that Drishti Samvedi of D17B has won 3rd prize at Department Technology Day, **Pradarshini '24** conducted on 22nd-23rd March 2024.

DR. MRS. NUPUR GIRI
HOD, COMPUTER DEPARTMENT

DR. MRS. GRESHA BHATIA
DHOD, COMPUTER DEPARTMENT

PROJECT COORDINATOR
COMPUTER DEPARTMENT

Vivekanand Education Society's Institute Of Technology, Mumbai

An Autonomous Institute affiliated to University of Mumbai, approved by AICTE

In association with VESIT - IQAC & VESIT - IIC

Department Of Computer Engineering

CERTIFICATE OF EXCELLENCE

This to certify that Vansh Pahuja
of D17A has won 3rd prize at Department
Technology Day, **Pradarshini '24**
conducted on 22nd-23rd March 2024.

DR. MRS. NUPUR GIRI	DR. MRS. GRESHA BHATIA	PROJECT COORDINATOR
HOD, COMPUTER DEPARTMENT	DHOD, COMPUTER DEPARTMENT	COMPUTER DEPARTMENT

Vivekanand Education Society's Institute Of Technology, Mumbai

An Autonomous Institute affiliated to University of Mumbai, approved by AICTE

In association with VESIT - IQAC & VESIT - IIC

Department Of Computer Engineering

CERTIFICATE OF EXCELLENCE

This to certify that Om Madat
of D17A has won 3rd prize at Department
Technology Day, **Pradarshini '24**
conducted on 22nd-23rd March 2024.

DR. MRS. NUPUR GIRI	DR. MRS. GRESHA BHATIA	PROJECT COORDINATOR
HOD, COMPUTER DEPARTMENT	DHOD, COMPUTER DEPARTMENT	COMPUTER DEPARTMENT