

ALTERNATIVE TO TRADITIONAL CREDENTIAL BASED AUTHENTICATION

A PROJECT REPORT

Submitted by,

Yeddula Nandini - 20201CSE0788

Sathela Haswitha- 20201CSE0791

Nafisa Fathima - 20201CSE0814

Chandana A.T - 20201CSE0820

Under the guidance of,

Ms. Rakheeba Taseen

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

At



PRESIDENCY UNIVERSITY

BENGALURU

JANUARY 2024

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project report “**ALTERNATIVE TO TRADITIONAL CREDENTIAL BASED AUTHENTICATION**” being submitted by “Yeddula Nandini, Sathela Haswitha, Nafisa Fathima, Chandana A.T” bearing roll number(s) “20201CSE0788, 20201CSE0791, 20201CSE0814, 20201CSE0820” in partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering is a Bonafide work carried out under my supervision.

Ms. Rakheeba Taseen

Assistant Professor
School of CSE&IS
Presidency University

Dr. Pallavi R

Associate Professor & HoD
School of CSE&IS
Presidency University

Dr. C. KALAIARASAN

Associate Dean
School of CSE&IS
Presidency University

Dr. L. SHAKKEERA

Associate Dean
School of CSE&IS
Presidency University

Dr. SAMEERUDDIN KHAN

Dean
School of CSE&IS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **ALTERNATIVE TO TRADITIONAL CREDENTIAL BASED AUTHENTICATION** in partial fulfilment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering**, is a record of our own investigations carried under the guidance of Rakhee Taseen, Assistant Professor, **School of Computer Science And Engineering, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

NAME	ROLL NUMBER	SIGNATURE
Yeddula Nandini	20201CSE0788	
Sathela Haswitha	20201CSE0791	
Nafisa Fathima	20201CSE0814	
Chandana A.T	20201CSE0820	

ABSTRACT

Traditional credential-based authentication methods, such as usernames and passwords, have long been the standard for securing digital systems and protecting sensitive information. However, the increasing sophistication of cyber threats and the proliferation of data breaches have highlighted the limitations of these conventional approaches. To address these challenges, researchers and practitioners have been exploring alternative authentication methods that offer enhanced security, usability, and privacy. This abstract aims to provide an overview of the emerging alternative approaches to traditional credential-based authentication. It discusses several innovative methods that leverage cutting-edge technologies and concepts to authenticate users in a more secure and user-friendly manner. Biometric authentication, for example, can be highly secure and convenient but may raise privacy concerns. Behavioral authentication, which analyzes a user's patterns of interaction with a system, can provide continuous authentication but may be difficult to implement effectively. Token-based authentication, such as one-time passwords, can provide an additional layer of security but may be cumbersome for users.

Keywords: Authentication, Usernames, Passwords, Secure.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Dean, School of Computer Science and Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We record our heartfelt gratitude to our beloved Associate Deans **Dr. Kalaiarasan C and Dr. Shakkeera L**, School of Computer Science and Engineering & Information Science, Presidency University and **Dr. Pallavi R**, Head of the Department, School of Computer Science and Engineering & Information Science, Presidency University for rendering timely help for the successful completion of this project.

We are greatly indebted to our guide **Ms. Rakheeba Taseen**, Assistant Professor School of Computer Science and Engineering & Information Science, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the University Project-II Coordinators **Dr. Sanjeev P Kaulgud, Dr. Mrutyunjaya MS** and the department Project Coordinators **“Mr. Md Ziaur Rahman , Dr. Thrimoorthy N”**.

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

Yeddula Nandini
Sathela Haswitha
Nafisa Fathima
Chandana A T

LIST OF TABLES

Sl. No.	Table Name	Table Caption	Page No.
1	Table 5.3.1	Admin Table	5
2	Table 5.3.2	New User Table	5
3	Table 5.3.3	New Bank Table	5

LIST OF FIGURES

Sl. No.	Figure	Caption	Page No.
1	Figure 5.1.1	UML diagram	12
2	Figure 5.1.2	Use case diagram	13
3	Figure 5.1.3	Data Flow Diagram	14
4	Figure 5.1	ER Diagrams	15-16
5	Figure 7.1	Gantt chart	21
6	Figure B1	Home page & Admin main page	31
7	Figure B2	Admin viewers & Admin view banks page	32
8	Figure B3	Admin view page & Main page	33
9	Figure B4	Authentication system app	34
10	Figure B5	Admin login page & User login page	34
11	Figure B6	User enter otp page	35
12	Figure B7	User main page	34
13	Figure B8	Kginfo Systems	36
14	Figure B9	Kginfo Systems New Sim Details	36
15	Figure B10	Kginfo Systems New Sim and Product Details	37
16	Figure B11	Kginfo Systems New Product Details	37
17	Figure B12	Kginfo Systems New Property Details	38

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	iv
	ACKNOWLEDGEMENT	v
01	INTRODUCTION	1-2
	1.1 Background of the Project	3
	1.2 Problem Context	4
	1.3 Objectives	5
02	LITERARTURE SURVEY	6-7
03	RESEARCH GAPS OF EXISTING METHODS	
	3.1 Use cases and implementation challenges	8
04	PROPOSED METHODOLOGY	
	4.1 Understanding MFA	9
	4.2 Factors of authentication	10
	4.3 MFA implementation best practices on traditional credential-based authentication	11
05	DESIGN AND IMPLEMENTATION	
	5.1 Design	12
	5.1.1 UML diagrams	12
	5.1.2 Use case diagrams	13
	5.1.3 Data flow diagram	14
	5.2 ER diagrams	15
	5.3 Implementation	17
	5.4 Data Tables	18
	5.3.1 Admin table	18
	5.3.2 New table	18
	5.3.3 New bank	18
06	BEHAVIOURAL BASED AUTHENTICATION	19
	6.1 Concept of behavioural based authentication	
	6.2 Behavioural authentication in practice on alternative to traditional credential-based authentication	
07	TIMELINE FOR EXECUTION OF PROJECT	20
08	OUTCOMES	
	8.1 Evaluation criteria	21
	8.2 Strengths and weakness	22
09	RESULTS AND DISCUSSIONS	23
	9.1 Adoption challenges and considerations	
	9.2 Organizational readiness	
	9.3 User acceptance	
	9.4 Privacy and legal concerns	
	9.5 Training and education	

10	CONCLUSION	24
	REFERENCES	25
	APPENDIX-A (PSEUDOCODE)	26-29
	APPENDIX-B (SCREENSHOTS)	30-36
	APPENDIX-C (ENCLOSURES)	37

CHAPTER-1

INTRODUCTION

In the rapidly evolving digital landscape of today, ensuring secure access to online services and valuable resources is crucial, and authentication plays a key role in achieving this. However, traditional authentication methods like usernames and passwords have proven to be limited and vulnerable to malicious exploitation by cyber threats, as technology advances. As a result, there is a strong drive to search for alternative authentication methods that not only improve security but also enhance the user experience. The main drawback of traditional credential-based authentication lies in the inherent weaknesses of passwords. Users often choose easily guessable or reused passwords, making them susceptible to brute force attacks or compromise in large-scale data breaches. Moreover, passwords can be forgotten or lost, leading to a frustrating user experience and necessitating complex recovery processes. Relying solely on passwords is no longer sufficient to adequately protect confidential information and digital assets. To address these concerns, various alternative authentication methods have emerged, aiming to enhance the authentication process through innovative technologies and concepts. One such method is biometrics, which utilizes an individual's unique physiological or behavioral characteristics such as fingerprints, facial features, or voice patterns to verify their identity. Biometric data is inherently difficult to duplicate or counterfeit, providing a high level of security. Additionally, biometric authentication eliminates the need for users to remember complex passwords, increasing convenience and reducing the likelihood of credential-related security breaches. Another promising approach in the authentication space is multi-factor authentication (MFA) or two factor authentication (2FA). This method combines multiple independent authentication factors to establish the user's identity, typically involving something the user knows (e.g., a password), something the user has (e.g., a smartphone or hardware token), or something the user is (e.g., a fingerprint or iris scan). By requiring multiple factors, MFA significantly enhances the security of the authentication process, as an attacker would need to compromise multiple elements to gain unauthorized access. In addition to biometrics and MFA, researchers are exploring other innovative authentication methods. Contextual authentication, for example considers contextual information such as location,

device, and behavioral patterns to assess the authenticity of access requests. Moreover, advancements in machine learning and artificial intelligence have led to the development of behavior-based authentication, where systems analyze user behavior patterns to detect anomalies and potential security threats. Biometrics offers a more secure and convenient approach to verify user identities as an alternative to traditional credential-based methods. This innovative authentication method leverages physical or behavioral characteristics that are unique to individuals, such as fingerprints, iris patterns, facial recognition, voice recognition, and even behavioral traits like key dynamics and gait analysis. The high level of security provided by biometrics stems from their inherent uniqueness, making it extremely difficult for attackers to duplicate or forge these traits. Biometrics are also challenging to tamper with or spoof, reducing the risks associated with stolen or compromised credentials. Furthermore, biometric authentication improves user convenience by eliminating the need to remember and manage multiple passwords. Users can authenticate themselves simply by providing their biometric traits, reducing the burden on users and enhancing the overall user experience. The versatility of biometric features allows for flexible implementation across various devices and services. For instance, fingerprint recognition is commonly used in smartphones and access control systems, while facial recognition finds applications in device unlocking and airport security. Speech recognition is employed in language assistants and telephone banking systems. This adaptability enables biometrics to cater to different user needs and use cases. Privacy concerns related to the storage and use of biometric data must be carefully addressed to ensure user trust and compliance with regulations. Additionally, the accuracy and reliability of biometric systems depend on factors such as sensor quality, environmental conditions, and the potential for spoofing attacks. These considerations emphasize the importance of implementing robust security measures and continuously evaluating and updating.

1.1 BACKGROUND OF THE PROJECT

In today's rapidly evolving digital landscape, authentication plays a crucial role in ensuring secure access to online services and valuable resources. However, traditional credential-based authentication methods, such as usernames and passwords, have become increasingly vulnerable to exploitation and are burdened with limitations. These challenges have led to the exploration and implementation of alternative authentication methods that not only enhance security but also improve the overall user experience. One of the primary drawbacks of traditional credential-based authentication is the reliance on passwords. Users face the daunting task of managing numerous login credentials across various online services. This complexity often leads to forgotten passwords, resulting in frustrating experiences and time-consuming recovery processes. Additionally, passwords are susceptible to being shared, guessed, or compromised in data breaches, further compromising the security of multiple accounts. To overcome these limitations, alternative authentication methods are being developed and deployed. These approaches aim to provide stronger security measures while addressing the user experience challenges associated with passwords. Biometric authentication is one such method that utilizes unique physiological or behavioral characteristics, such as fingerprints, facial features, or voice patterns, to verify user identities. Biometrics offer a higher level of security as they are inherently difficult to duplicate or forge.

1.2 PROBLEM CONTEXT

The conventional method of credential-based authentication, which relies on usernames and passwords, faces substantial challenges due to its susceptibility to different types of attacks. Attackers exploit the weaknesses inherent in this authentication method, including the use of weak passwords, phishing attempts, brute force attacks, and credential stuffing. These attacks can have severe consequences, ranging from compromised user accounts and financial losses to invasions of privacy and reputational harm for individuals and organizations. One significant risk lies in the use of weak passwords by many users. Commonly chosen passwords, such as easily guessable words or sequential numbers, pose a considerable security threat. Attackers can employ brute force techniques to systematically guess passwords until they find the correct one. Moreover, credential stuffing attacks take advantage of compromised credentials from one service to gain unauthorized access to other accounts where users have reused passwords. Phishing attacks represent another major threat to traditional authentication. In such attacks, malicious actors impersonate trusted entities and send deceptive emails or messages to trick users into divulging their authentication information. Stolen credentials obtained through phishing can be used to gain unauthorized access to user accounts and confidential information. Additionally, attackers can intercept credentials by eavesdropping on insecure networks or exploiting vulnerabilities in the authentication process. Techniques like man-in-the-middle attacks enable attackers to intercept and modify communications between users and legitimate servers, thus obtaining usernames, passwords, or other authentication tokens. The consequences of a compromised user account extend beyond financial losses. Attackers can gain access to personal, financial, and sensitive business data, leading to data breaches and exposing individuals and organizations to identity theft and corporate espionage. Furthermore, unauthorized access to user accounts can serve as a launching point for further attacks within a system or network. To address these vulnerabilities, alternative authentication methods have been developed and implemented.

1.3 OBJECTIVES

The 4 main objectives for this project:

- Examine various alternatives to traditional username and password authentication: This involves conducting a comprehensive study of alternative authentication methods that have emerged as a response to the shortcomings of password-based systems. Examples of such methods include biometrics, multi-factor authentication, contextual authentication, behavior-based authentication, and other innovative approaches.
- Assess the advantages and disadvantages of each alternative method: The aim is to conduct a thorough analysis and evaluation of the strengths and weaknesses of each alternative authentication method. Factors such as security, ease of use, scalability, compatibility with existing systems, and potential implementation challenges are carefully examined to gain a comprehensive understanding of each approach.
- Evaluate the feasibility and usability of alternative authentication approaches: This objective focuses on evaluating the practicality and usability of alternative authentication methods. It entails considering technical requirements, infrastructure considerations, the impact on user experience, and potential deployment scenarios in different contexts, such as enterprise environments, online services, and mobile applications. The aim is to identify any barriers that may hinder the adoption of these alternative methods
- Assess the safety impact and effectiveness of these alternatives: Security is of utmost importance in any authentication system. This objective involves evaluating the security impact of each alternative method, including their resilience against various attacks and their ability to protect against emerging threats. The effectiveness of these methods in safeguarding user accounts, sensitive data, and digital assets is carefully studied

CHAPTER-2

LITERATURE SURVEY

Traditional credential-based authentication is a commonly employed approach for verifying the identity of individuals seeking access to systems, applications, or services. This method relies on the use of credentials, typically in the form of usernames and passwords, as a means of authenticating users. The user furnishes their credentials, encompassing a username and password, as input. The system undertakes the verification of the provided credentials, cross-referencing them against stored credentials associated with the user's account. In the event of a successful match between the provided and stored credentials, the user is granted permission to access the system, application, or service in question. This conventional approach to authentication has been widely adopted due to its simplicity and familiarity to users. However, it is crucial to acknowledge that it also possesses inherent vulnerabilities and limitations, which have necessitated the exploration and development of alternative authentication methods to address these concerns.

Traditional authentication methods face several limitations and challenges that undermine their effectiveness and security. These include:

- **Weak Passwords:** Users commonly select easily guessable or simple passwords, such as common words or basic combinations. This vulnerability makes it easier for attackers to exploit and gain unauthorized access to user accounts.
- **Password Reuse:** Many individuals tend to reuse passwords across multiple accounts. This practice amplifies the risk of credential compromise. If one account is breached, it provides attackers with access to other accounts where the same password is used.
- **Forgotten Passwords:** Users frequently forget their passwords, resulting in account lockouts and the need for password resets. This situation inconveniences both users and system administrators, leading to frustration and additional support overhead.
- **Social Engineering:** Attackers employ social engineering techniques, such as phishing or impersonation, to exploit human vulnerabilities and deceive users into revealing their credentials. These tactics manipulate individuals into unknowingly divulging sensitive Information.
- **Credential Theft:** Passwords can be stolen through various means, including data breaches, keyloggers, or malware. Once obtained, these compromised credentials are exploited by attackers to gain unauthorized access to systems, applications, or services. Addressing these limitations requires the adoption of alternative authentication methods that enhance security and mitigate these vulnerabilities.
- **By exploring innovative approaches such as biometrics, multi-factor authentication, or contextual authentication, organizations can establish stronger safeguards and provide users with a more secure and streamlined authentication experience.**

Biometric authentication offers several advantages over traditional credential-based methods, including:

- **Enhanced security:** Biometric traits are unique to everyone, making it extremely difficult for attackers to replicate or forge them. This enhances the security of authentication systems and protects against unauthorized access.
- **Convenience:** Biometric authentication eliminates the need for users to remember and manage complex passwords or credentials. Users simply need to provide their biometric data, making the authentication process more convenient and user friendly.
- **Non-transferability:** Biometric traits are inherently tied to the individual and cannot be easily shared or stolen. Unlike passwords or tokens, which can be transferred, biometric data remains closely linked to the person, reducing the risk of credential sharing or theft.
- **Speed and efficiency:** Biometric authentication is often quick and seamless. Users can access systems or services with a simple scan or verification, saving time and improving overall efficiency.

CHAPTER-3

RESEARCH GAPS OF EXISTING METHODS

3.1 USE CASES AND IMPLEMENTATION CHALLENGES:

Biometric authentication is widely applicable across various domains, including:

- ❖ **Mobile devices:** Biometric features such as fingerprint or facial recognition are commonly used in smartphones and tablets for convenient device unlocking and secure transaction Authorization.
- ❖ **Border control and airports:** Biometric systems play a crucial role in identity verification at immigration checkpoints and airport security. They enable efficient and accurate matching against watchlists to enhance border security.
- ❖ **Financial institutions:** Biometric authentication is employed by banks and financial institutions to provide secure access to banking services, authorize ATM transactions, and enhance payment security.
- ❖ **Physical access control:** Biometric systems are used for granting access to secure areas within buildings, data centers, or high-security facilities. This ensures that only authorized individuals can enter restricted areas. While biometric authentication offers numerous benefits, there are also certain challenges associated with its implementation.
- ❖ **Cost:** Implementing biometric systems can involve significant expenses, including acquiring the necessary hardware, integrating the system into existing infrastructure, and ongoing maintenance and support.
- ❖ **Standardization:** Achieving standardization and interoperability between different biometric systems and devices can be challenging. Ensuring seamless integration and compatibility across various platforms and technologies remains an ongoing effort.

CHAPTER-4

PROPOSED METHODOLOGY

4.1 UNDERSTANDING MFA:

- ◆ Multi-Factor Authentication (MFA), also referred to as Two-Factor Authentication (2FA), is a robust security measure designed to enhance the authentication process by requiring users to provide multiple independent factors of identification.
- ◆ MFA requires users to present two or more different types of authentication factors during the login process. These factors fall into three categories: something the user knows (such as a password or PIN), something the user has (such as a physical token or smartphone), and something the user is (such as a biometric trait like a fingerprint or facial recognition).
- ◆ The purpose of MFA is to address the limitations and vulnerabilities of relying solely on passwords for authentication. Since passwords can be compromised through brute-force attacks, phishing, or other means, MFA acts as a safeguard by introducing additional barriers for unauthorized individuals attempting to gain access to user accounts or sensitive information.
- ◆ By requiring multiple authentication factors, MFA adds complexity to the authentication process and makes it significantly more difficult for attackers to impersonate legitimate users. Even if an attacker manages to obtain or guess a user's password, they will still need to provide the additional required factor(s) to successfully authenticate.
- ◆ MFA has become increasingly prevalent across various digital platforms, including online services, banking systems, cloud applications, and more. Its implementation helps protect user accounts, mitigate the risks associated with weak or compromised passwords, and strengthens overall security posture.

4.2 FACTORS OF AUTHENTICATION:

- Multi-Factor Authentication (MFA) is a security measure that strengthens the authentication process by combining three distinct factors of identification. These factors include the knowledge factor, possession factor, and inherence factor, collectively working together to provide a robust layer of security.
- The knowledge factor pertains to information that the user knows, such as a password, a personal identification number (PIN), or the correct answers to specific security questions. It involves the user's ability to recall and provide confidential information that is unique to them.
- The possession factor relates to something that the user possesses physically. This can include a physical token, a smart card, or a mobile device that generates one-time passwords (OTP). The user must possess the authorized item or device to successfully complete the authentication process.
- The inherence factor involves characteristics inherent to the user themselves. This factor encompasses biometric traits, such as fingerprints or facial recognition, as well as behavioral characteristics like voice recognition or typing patterns. These traits are unique to each individual and difficult to forge or replicate.
- By combining two or more of these factors during the authentication process, MFA significantly enhances security. The multi-layered approach makes it more challenging for attackers to gain unauthorized access since they would need to compromise multiple factors instead of relying solely on a password.

4.3 MFA Implementation Best Practices on Traditional Credential-Based Authentication:

When implementing MFA in traditional credential-based authentication systems, consider the following best practices:

- **Assess risk and select appropriate factors:** Evaluate the sensitivity of the systems and data being protected and choose the most appropriate combination of factors. For example, high-security systems may require a combination of a password and a physical token or biometric factor.
- **Provide a range of authentication options:** Offer users multiple MFA methods to choose from, such as SMS-based OTP, authenticator apps, hardware tokens, or biometric authentication, based on their preferences and device capabilities.
- **Educate users:** Provide clear instructions and education on how to set up and use MFA. Explain the benefits and importance of MFA in enhancing security and protecting their accounts.
- **Consider fallback options:** In case a user loses or forgets their additional factor, provide alternative authentication methods or temporary access to prevent lockouts.
- **Regularly review and update MFA settings:** Periodically review and update MFA settings, including enforcing MFA for high-risk accounts or critical systems, and deactivating unused or outdated authentication methods.
- **Monitor and respond to MFA events:** Implement monitoring and logging capabilities to detect and respond to any MFA-related events, such as failed authentication attempts or suspicious activity
- **This project involves comparing the performance of various machine learning algorithms to determine the most effective approach for heart disease prediction.**

CHAPTER-5

DESIGN AND IMPLEMENTATION

5.1 DESIGN

Design is the first step in the development phase for any techniques and principles for defining a device, a process or system in sufficient detail to permit its physical realization. Once the software requirements have been analyzed and specified the software design involves three technical activities - design, coding, implementation and testing that are required to build and verify the software. Design activities are of main importance in this phase, because in this activity, decisions ultimately affecting the success of the software implementation and its ease of maintenance are made. These decisions have the final bearing upon reliability and maintainability of the system.

5.1.1 UML DIAGRAMS

Actor:

A coherent set of roles that users of use cases play when interacting with the use cases.



Fig 5.1.1 Actor diagram

Use case:

A description of sequence of actions, including variants, that a system performs that yield an observable result of value of an actor.



Fig 5.1.1 Use case diagram

5.1.2 USE CASE DIAGRAMS

A Use case is a description of a set of sequence of actions. Graphically it is rendered as an ellipse with solid line including only its name. A use case diagram is a behavioral diagram that shows a set of use cases and actors and their relationship. It is an association between the use cases and actors. An actor represents a real-world object. Primary Actor – Sender, Secondary Actor Receiver.

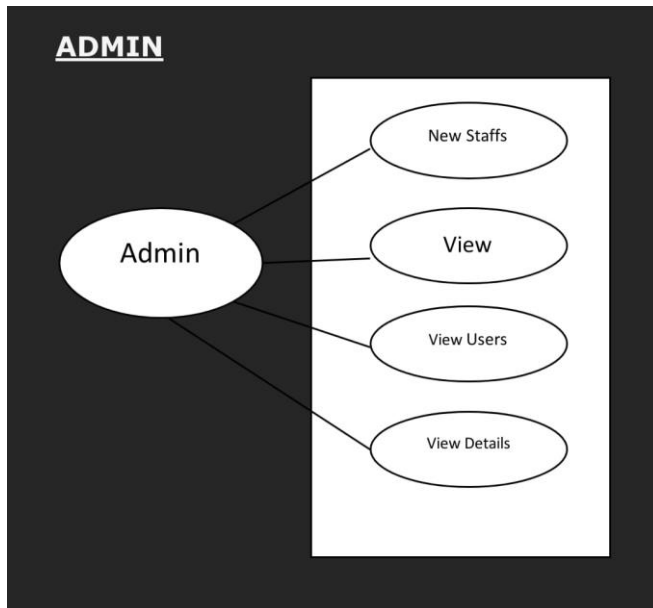


Fig 5.1.1 Admin diagram

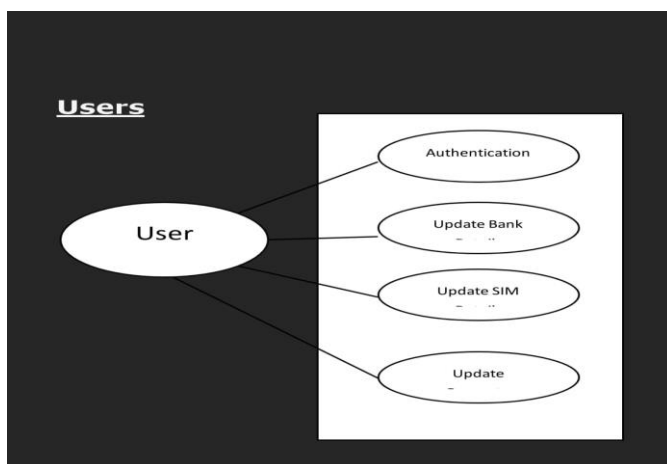


Fig 5.1.2 user diagram

5.1.3 DATA FLOW DIAGRAMS

The DFD takes an input-process-output view of a system i.e. data objects flow into the software, are transformed by processing elements, and resultant data objects flow out of the Software.

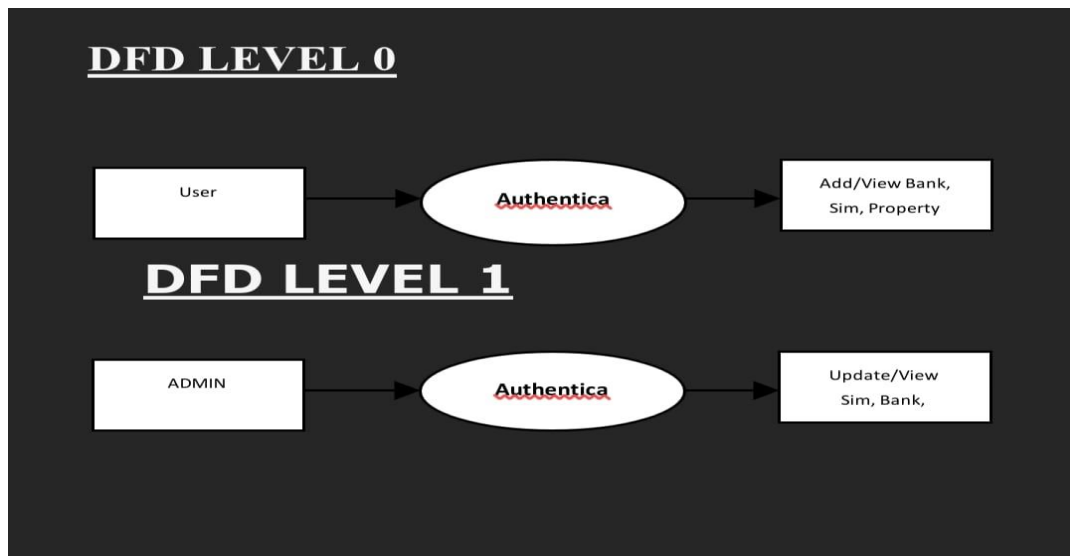


Fig 5.1.3 data flow diagram

5.2 ER DIAGRAMS

The Entity-Relationship (ER) model was originally proposed by Peter in 1976 [Chen76] to unify the network and relational database views. Simply stated the ER model is a conceptual data model that views the real world as entities and relationships. A basic component of the model is the Entity-Relationship diagram which is used to visually represent data objects.

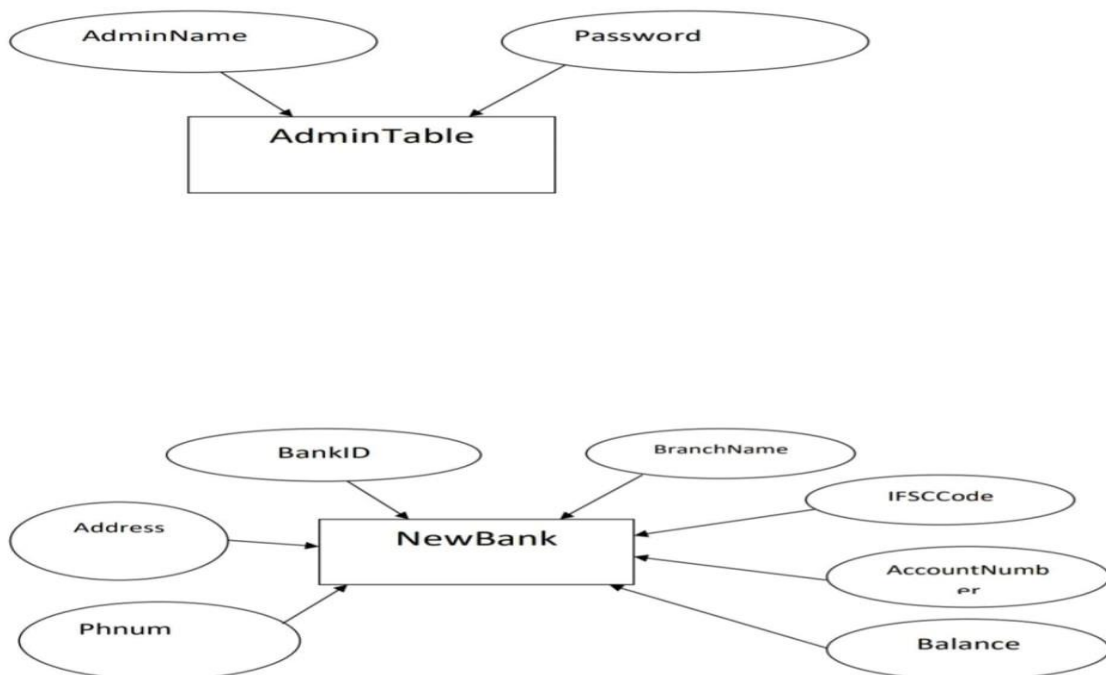


Fig 5.2 Admin and bank table

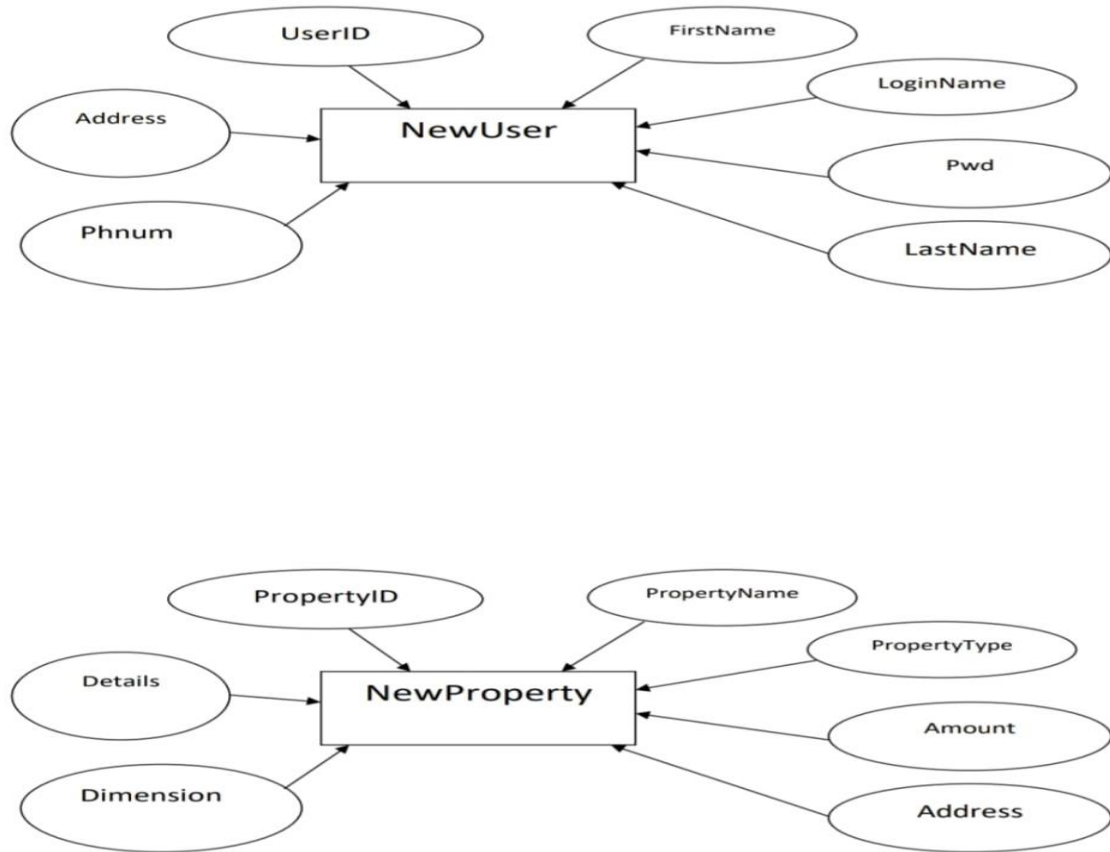


Fig 5.2 user and property table

5.3 IMPLEMENTATION

Implementation is the stage where the theoretical design is turned into a working system. The most crucial stage in achieving a new successful system and in giving confidence in the new system for the users that it will work efficiently and effectively. The system can be implemented only after thorough testing is done and if it is found to work according to the specification. It involves careful planning, investigation of the current system and its constraints on implementation, design of methods to achieve the changeover and an evaluation of change over methods apart from planning. Two major tasks of preparing the implementation are education and training of the users and testing of the system. The more complex the system being implemented, the more involved will be the systems analysis and design effort required just for implementation. The implementation phase comprises of several activities. The required hardware and software acquisition is carried out. The system may require some software to be developed. For this, programs are written and tested. The user then changes over to his new fully tested system and the old system is discontinued.

5.4 Data Tables

5.3.1 Admin Table

Field	Type
Admin Name	varchar (20)
Password	varchar (20)

5.3.2 New User Table

Field	Type	Null
User Id	int (11)	NO
First Name	varchar (50)	YES
Last Name	varchar (50)	YES
Phone Num	varchar (50)	YES
Email ID	varchar (50)	YES
U name	varchar (50)	YES
Pwd	varchar (50)	YES

5.3.3 New Bank Table

Field	Type	Null
Bank Id	int (11)	NO
Bank Name	varchar (50)	YES
Branch Name	int (11)	YES
Address	varchar (50)	YES
IFSC Code	varchar (50)	YES
Account Number	varchar (50)	YES

CHAPTER-6

BEHAVIOURAL BASED AUTHENTICATION

6.1 CONCEPT OF BEHAVIORAL-BASED AUTHENTICATION:

Behavioral-based authentication is an alternative authentication method that leverages individual's unique behavioral patterns to verify their identity. It focuses on capturing and analyzing various behavioral aspects of users, such as their typing patterns, mouse movements, touchscreen gestures, voice characteristics, and even their cognitive responses. By creating a profile of an individual's behavioral traits, this authentication method aims to distinguish legitimate users from impostors based on their consistent behavioral patterns.

6.2 BEHAVIORAL AUTHENTICATION IN PRACTICE ON ALTERNATIVE TO TRADITIONAL CREDENTIAL-BASED AUTHENTICATION:

- Implementing behavioral-based authentication as an alternative to traditional credential-based authentication involves several steps:
- Data Collection: Gather behavioral data from users by recording their interactions, such as typing patterns, mouse movements, touchscreen gestures, or voice samples.
- Behavioral Profiling: Analyze the collected data to build user profiles that represent their unique behavioral patterns. Machine learning techniques can be employed to identify and extract relevant features from the data.
- Real-Time Authentication: During the authentication process, compare the current user behavior with their stored profile. Use algorithms to determine if the behavior matches the legitimate user's patterns.

- Risk Assessment: Assign risk scores based on the degree of behavioral deviation from the user's profile. Higher deviations may trigger additional authentication measures or raise alerts for suspicious activity.

CHAPTER-7

7.1 TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)

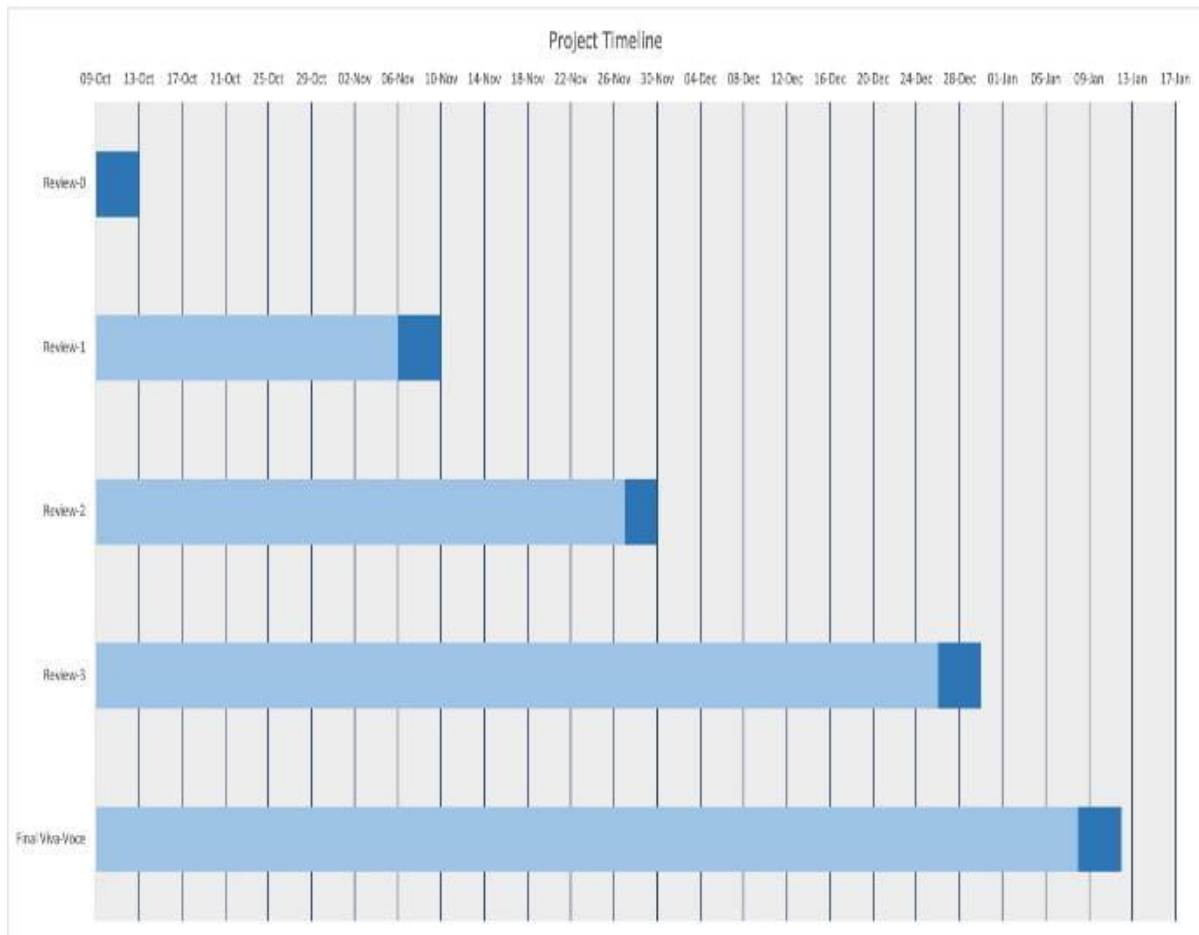


Figure7.1 Gantt chart

CHAPTER-8

OUTCOMES

8.1 EVALUATION CRITERIA:

To conduct a comparative analysis of alternative authentication methods to traditional credential-based authentication, we can consider the following evaluation criteria:

- Security: The effectiveness of each method in providing robust security and protecting against various attack vectors.
- User Experience: The convenience, ease of use, and user satisfaction with each authentication method.
- Scalability: The ability to implement authentication methods across various systems, platforms, and user populations.
- Implementation Complexity: The level of complexity involved in deploying and integrating the authentication method into existing systems.
- Cost: The financial implications, including initial setup costs, maintenance expenses, and any additional hardware or software requirements.
- Privacy: The impact on user privacy and the handling of sensitive biometric or personal data.
- Reliability: The reliability and availability of the authentication method, including factors such as system uptime and resilience to system failures.

8.2 STRENGTHS AND WEAKNESSES:

Biometric authentication

Strengths: Enhanced security through unique biometric traits, convenience for users, non-transferability of biometric data.

Weaknesses: Privacy concerns, accuracy issues, implementation complexity, revocability challenges.

Multi-Factor Authentication (MFA)

Strengths: Increased security through multiple authentication factors, protection against credential theft, flexibility for users.

Weaknesses: Implementation complexity, user resistance, dependency on additional factors, potential for inconvenience.

Password less Authentication

Strengths: Improved security by eliminating passwords, convenience for users, reduced risk of password-related issues.

Weaknesses: Adoption challenges, compatibility with existing systems, potential reliance on alternative factors like biometrics or devices.

CHAPTER-9

RESULTS AND DISCUSSIONS

9.1 ADOPTION CHALLENGES AND CONSIDERATIONS:

When implementing alternative authentication methods, organizations need to address several challenges and considerations.

9.2 ORGANIZATIONAL READINESS:

Ensure that the organization's infrastructure, systems, and processes are ready to support the chosen authentication method.

9.3 USER ACCEPTANCE:

Consider user acceptance and potential resistance to changes in authentication methods. User education and communication are crucial to promote understanding and acceptance.

9.4 PRIVACY AND LEGAL CONCERNS:

Address privacy and legal considerations, especially when dealing with biometric or personal data. Compliance with relevant regulations and policies is essential.

9.5 TRAINING AND EDUCATION:

Provide adequate training and education to users on how to use the new authentication method, its benefits, and any changes to the authentication process.

CHAPTER-10

CONCLUSION

Traditional credential-based authentication has been widely used for many years, but it has several limitations and challenges. Weak passwords, password reuse, and forgotten passwords are common issues that lead to security vulnerabilities. Social engineering attacks and credential theft further exacerbate the risks associated with traditional authentication methods. User inconvenience and password fatigue are also significant drawbacks of traditional credential-based authentication. Users struggle to remember complex passwords for multiple accounts, leading to frustration and potential security risks. Regular password changes and the introduction of two-factor authentication (2FA) add further complexity and inconvenience for users. To address the shortcomings of traditional authentication, alternative methods such as biometric authentication, multi-factor authentication (MFA), and password less authentication have emerged. These methods offer enhanced security, convenience, and reduced reliance on passwords. Biometric authentication leverages unique physiological or behavioral traits for identity verification, while MFA combines multiple factors of authentication to provide an extra layer of security. These approaches mitigate the weaknesses of traditional credential-based authentication and offer better protection against attacks. However, it is important to consider the advantages and limitations of each authentication method and choose the most suitable approach based on the specific security requirements and user needs. Implementing best practices and staying updated with evolving authentication technologies and threats is crucial to maintaining a robust authentication system. Overall, traditional credential-based authentication has its place, but it is increasingly important to adopt more secure and user-friendly authentication methods to address the ever-evolving landscape of cybersecurity threats.

REFERENCES

- [1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. New York: Wiley, 2008
- [2] R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in Graphical Authentication," *Int. J. Secure. Its Appl.*, vol. 7, no. 3, pp. 347–356, 2013.
- [3] K. I. P. Patil and J. Shimpi, "A Graphical Password using Token, Biometric, Knowledge Based Authentication System for Mobile Devices," *Int. J. Innova. Technol. Explore. Eng.*, vol. 2, no. 4, pp. 155–157, 2013.
- [4] A. H. Lashkari, S. Farmand, D. O. Bin Zakaria, and D. R. Saleh, "Shoulder Surfing attack in graphical password authentication," *Int. J. Compute. Sci. Inf. Secure.*, vol. 6, no. 2, p. 10, Dec. 2009.
- [5] K. Renaud, "On user involvement in production of images used in visual authentication," *J. Vis. Lang. Compute.*, vol. 20, no. 1, pp. 1–15, Feb. 2009
- [6] National Academy of Sciences; Royal Society, *Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum*. The National Academies Press, 2015.
- [7] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google," pp. 141–150, May 2015.
- [8] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A Comprehensive Security Assessment," *IEEE Secur. Priv. Mag.*, vol. 8, no. 2, pp. 35–44, Mar. 2010.
- [9] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In search of usable security: five lessons from the field," *IEEE Secur. Priv. Mag.*, vol. 2, no. 5, pp. 19–24, Sep. 2004
- [10] A. Rabkin, "Personal knowledge questions for fallback authentication," in *Proceedings of the 4th symposium on Usable privacy and security - SOUPS '08*, 2008, p. 13.

APPENDIX-A

PSUEDOCODE

MainActivity.xml

```
<?xml version="1.0" encoding="utf-8"?>
<RelativeLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:app="http://schemas.android.com/apk/res-auto"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    tools:context=". Main Activity">
    <ScrollView
        android:layout_width="match_parent"
        android:layout_height="match_parent">
        <LinearLayout
            android="@+id/layout button"
            android:orientation="vertical"
            android:layout_alignParentTop="true"
            android:weightSum="2"
            android:layout_width="match_parent"
            android:layout_height="wrap_content">
            <TextView
                android:layout_width="wrap_content"
                android:layout_height="wrap_content"
                android:layout_centerHorizontal="true"
                android:layout_gravity="center_horizontal"
```

```
android:layout_marginTop="50dp"
android:text="Authetication System App"
android:textSize="40dp"
android:gravity="center"
android:textStyle="bold"
/>
<ImageView
android:id="@+id/imageView"
android:layout_width="match_parent"
android:layout_height="200dp"
app:srcCompat="@drawable/authenticationlogo" />
<Button
android:id="@+id/startappbtn"
android:layout_width="match_parent"
android:layout_height="75dp"
android:layout_marginStart="10dp"
android:layout_marginLeft="50dp"
android:layout_marginTop="50dp"
android:layout_marginEnd="10dp"
android:layout_marginBottom="10dp"
android:background="@drawable/shapesignup"
android:shadowColor="@android:color/transparent"
android:text="Start App"
android:textColor="@color/white" />
<Button
android:id="@+id/exitbtn"
android:layout_width="match_parent"
android:layout_height="75dp"
android:layout_marginStart="10dp"
android:layout_marginLeft="50dp"
android:layout_marginTop="50dp"
android:layout_marginEnd="10dp"
android:layout_marginBottom="10dp"
android:background="@drawable/shapesignup"
android:shadowColor="@android:color/transparent"
android:text="Exit"
android:textColor="@color/white" />
</LinearLayout>
</ScrollView>
</RelativeLayout>
```

MainActivity.java

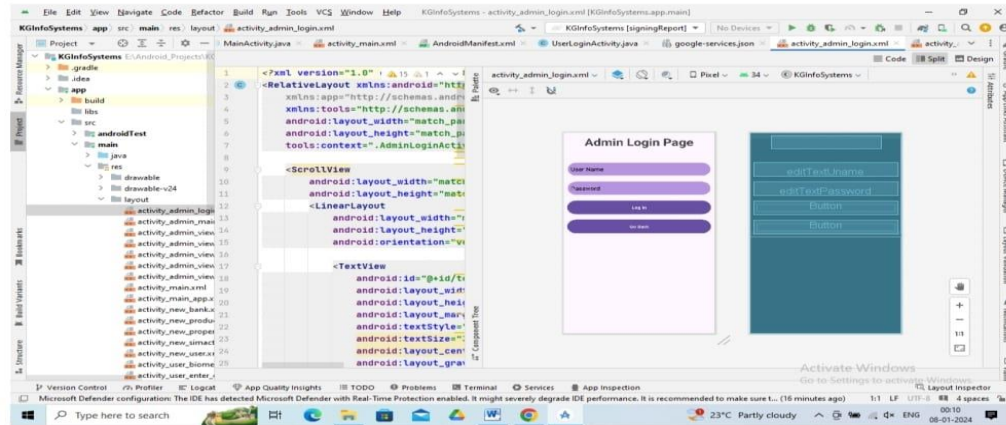
```
package com.example.kinfosystems;
import androidx.appcompat.app.AppCompatActivity;
import android.app.ProgressDialog;
import android.content.Intent;
import android.graphics.Bitmap;
import android.graphics.Color;
import android.graphics.drawable.ColorDrawable;
import android.net.Uri;
import android.provider.MediaStore;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.ImageView;
import android.widget.Toast;
import java.io.IOException;
import java.util.UUID;
import android.os.Bundle;
import android.widget.Button;
import androidx.appcompat.app.AppCompatActivity;
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import androidx.annotation.NonNull;
import androidx.appcompat.app.ActionBarDrawerToggle;
import androidx.appcompat.app.AppCompatActivity;
import androidx.drawerlayout.widget.DrawerLayout;
import android.os.Bundle;
import android.view.MenuItem;
import android.app.ProgressDialog;
import android.content.Intent;
import android.graphics.Bitmap;
import android.graphics.Color;
import android.graphics.drawable.ColorDrawable;
import android.net.Uri;
import android.provider.MediaStore;
import android.os.Bundle;
import android.view.View;
```

```
import android.widget.Button;
import android.widget.ImageView;
import android.widget.Toast;
import com.google.android.gms.tasks.OnFailureListener;
import com.google.android.gms.tasks.OnSuccessListener;
import com.google.firebase.firestore.FirebaseFirestore;
import com.google.firebase.storage.FirebaseStorage;
import com.google.firebase.storage.OnProgressListener;
import com.google.firebase.storage.StorageReference;
import com.google.firebase.storage.UploadTask;
import java.io.IOException;
import java.util.UUID;
public class MainActivity extends AppCompatActivity {
private Button startappbtn,exitBtn;
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        startappbtn=(Button)findViewById(R.id.startappbtn);
        exitBtn = (Button) findViewById(R.id.exitbtn);
        startappbtn.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                Intent intent = new Intent(getApplicationContext(), MainAppActivity.class);
                startActivity(intent);
            }
        });
        exitBtn.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                MainActivity.this.finish();
                finishAffinity();
            }
        });
    }
}
```

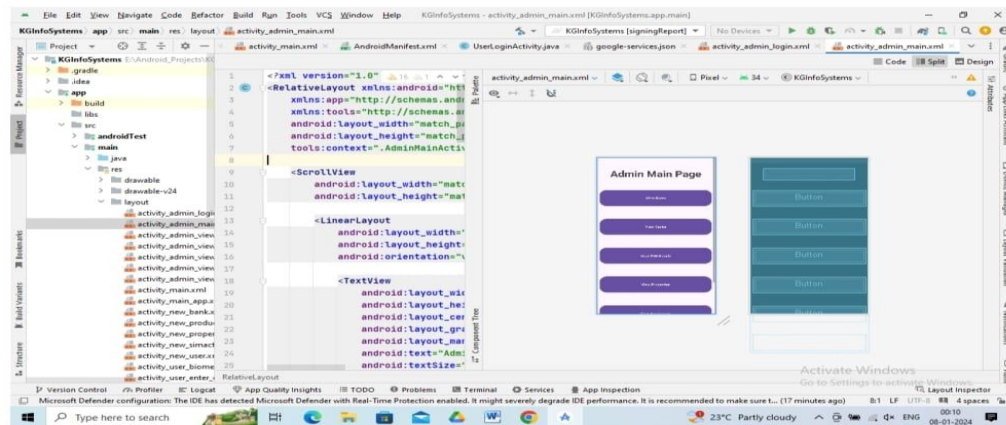
APPENDIX-B

SCREENSHOTS

Homepage

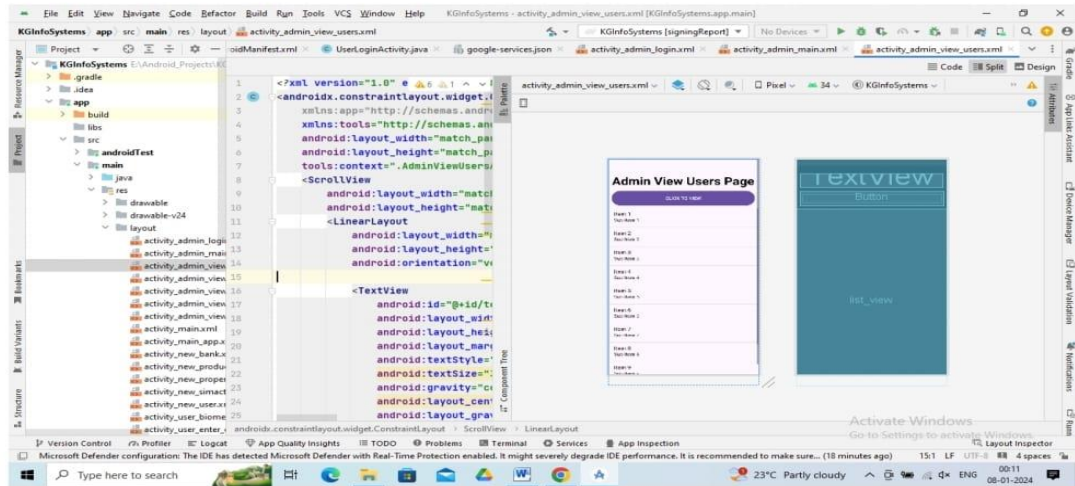


AdminMainPage

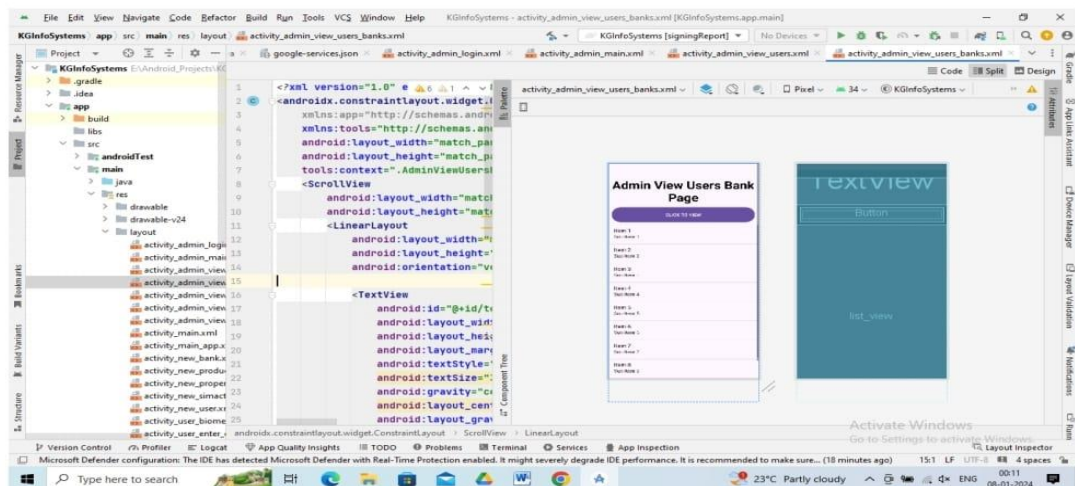


B1Figure: Home and Admin page

Adminviewusers



Adminviewbankspage

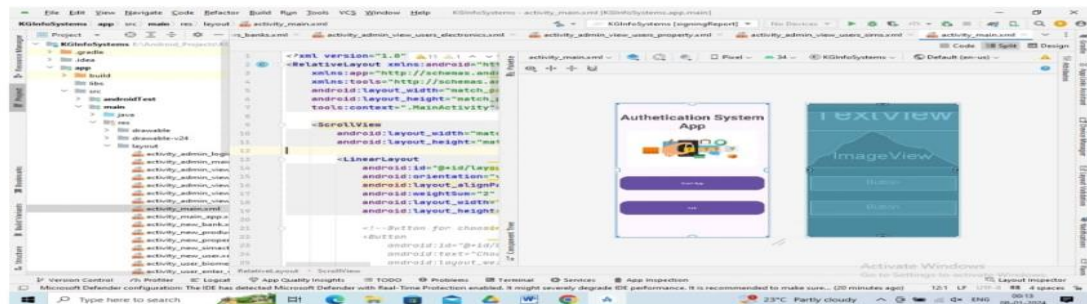


B2 Figure: Admin view user and bank page

Adminviewsimpage



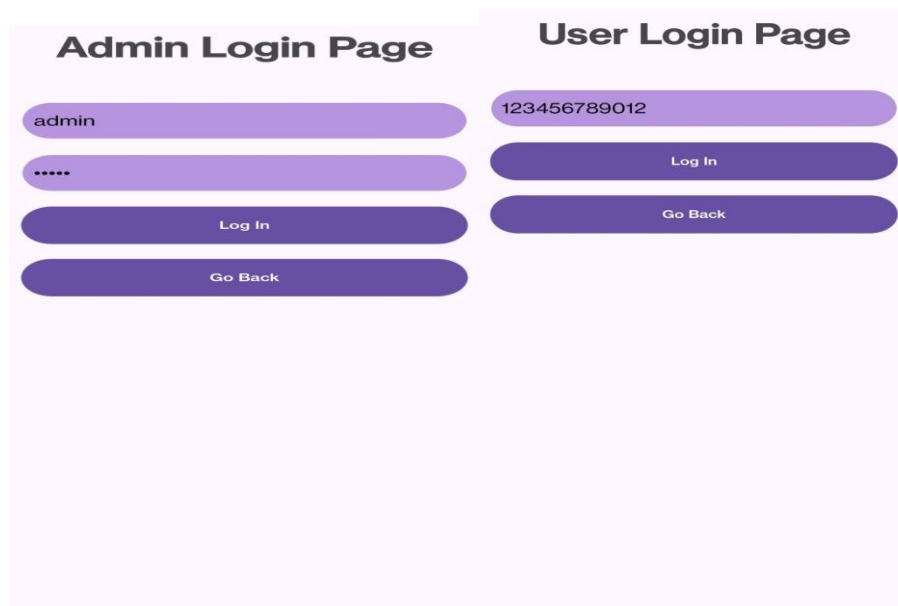
MainPage



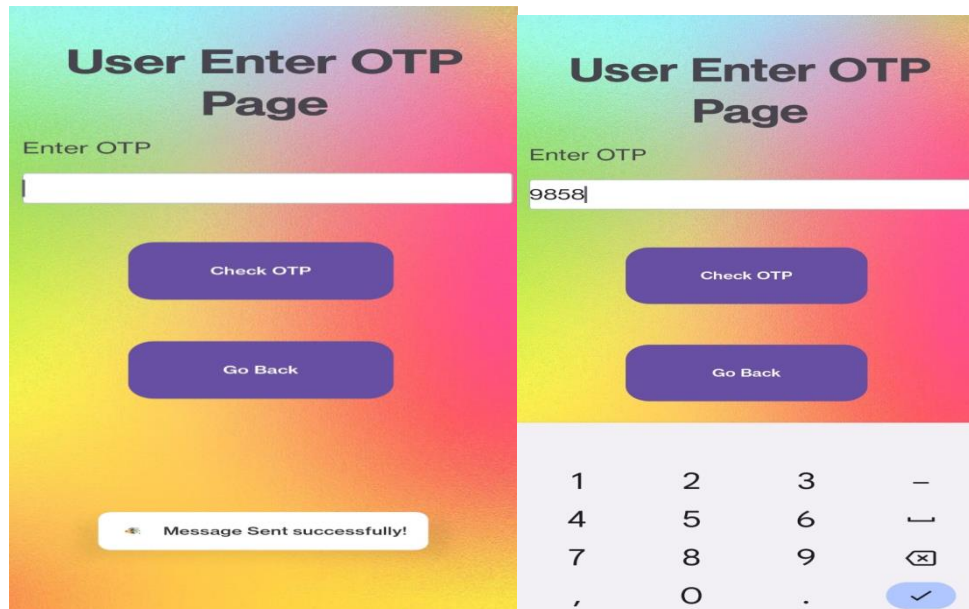
B3 Figure: Admin view sim and main page



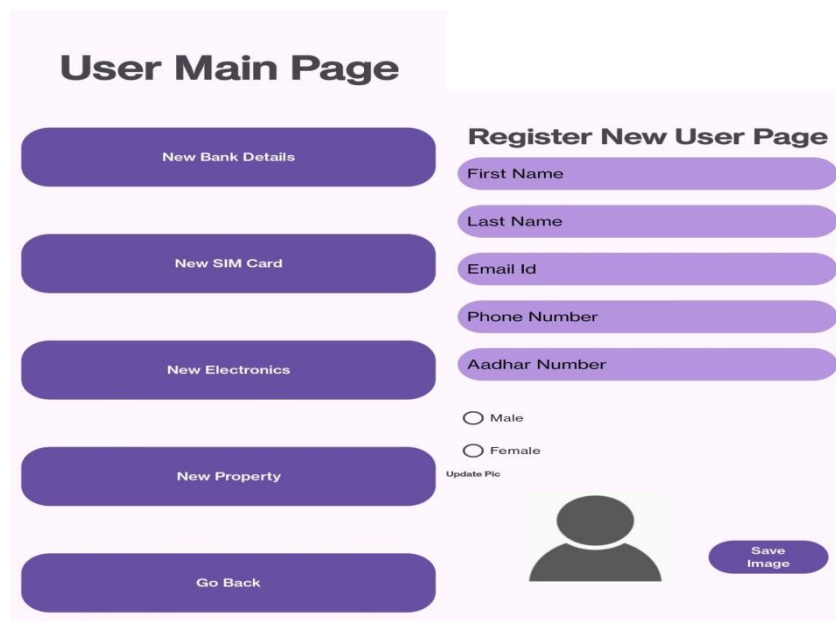
B4 Figure: Authentication System App



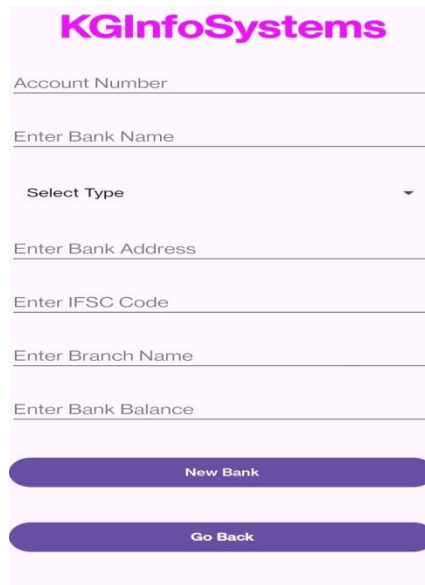
B5 Figure: Admin login page and User login page



B6 Figure: User enter otp page



B7 Figure: User main page



KGInfoSystems

Account Number

Enter Bank Name

Select Type

Enter Bank Address

Enter IFSC Code

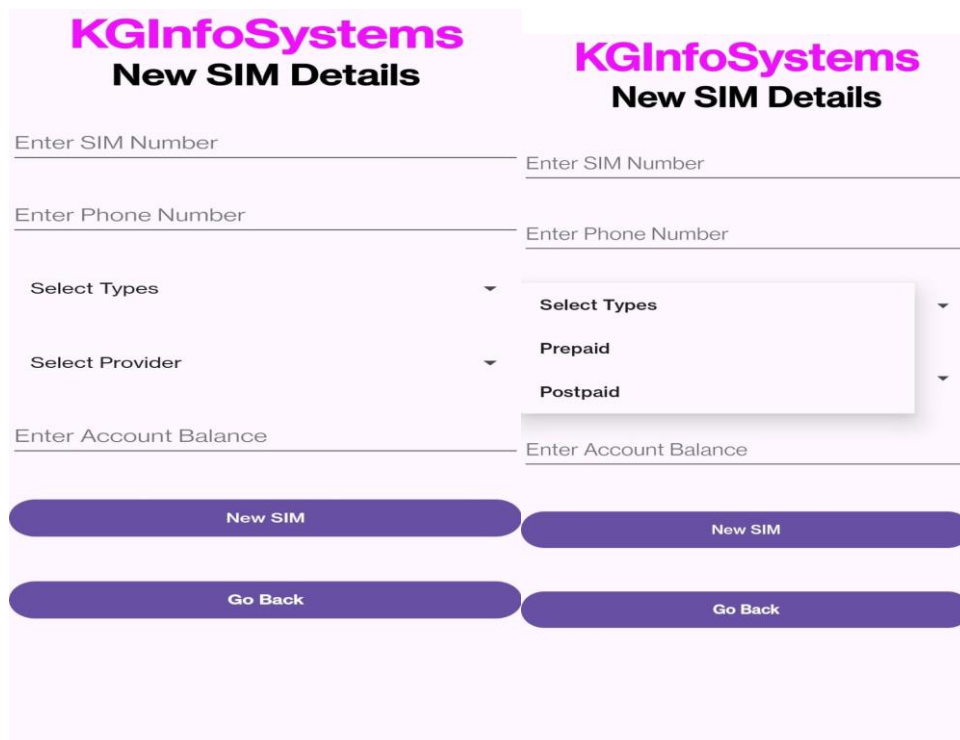
Enter Branch Name

Enter Bank Balance

New Bank

Go Back

B8 Figure: Kg Info Systems



KGInfoSystems
New SIM Details

Enter SIM Number

Enter Phone Number

Select Types

Select Provider

Enter Account Balance

New SIM

Go Back

KGInfoSystems
New SIM Details

Enter SIM Number

Enter Phone Number

Select Types

Prepaid

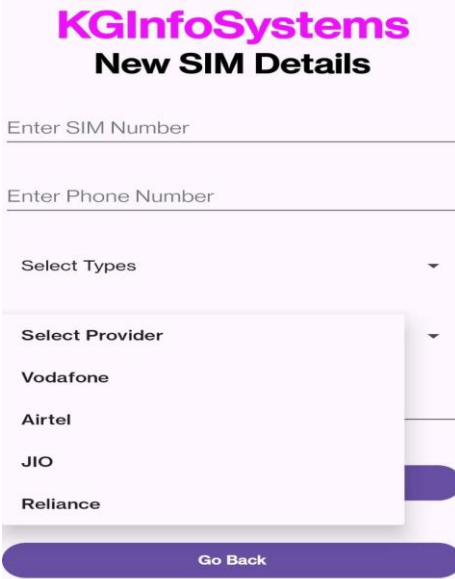
Postpaid

Enter Account Balance

New SIM

Go Back

B9 Figure: Kg Info Systems Sim Details



KGInfoSystems
New SIM Details

Enter SIM Number

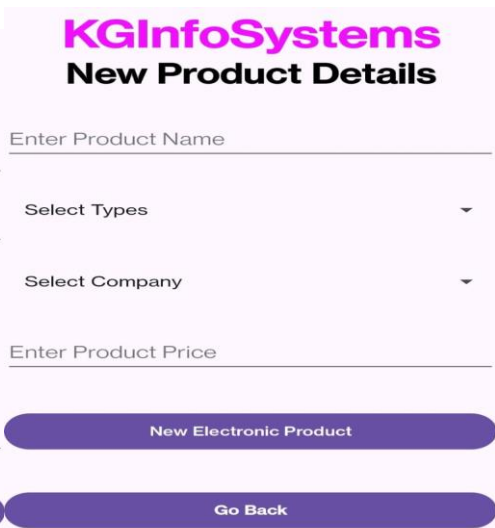
Enter Phone Number

Select Types

Select Provider

- Vodafone
- Airtel
- JIO
- Reliance

Go Back



KGInfoSystems
New Product Details

Enter Product Name

Select Types

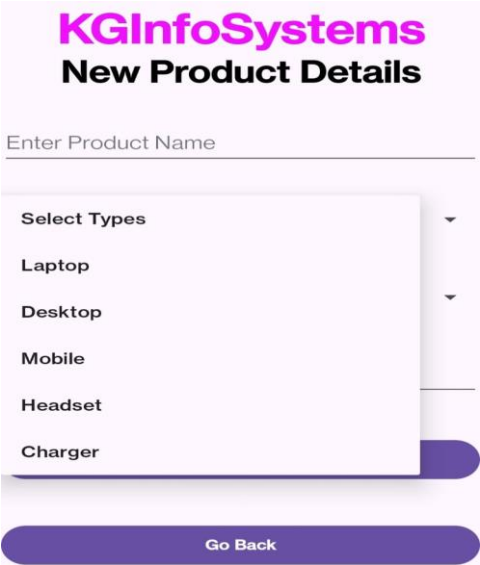
Select Company

Enter Product Price

New Electronic Product

Go Back

B10 Figure: Kg info Systems New Product Details



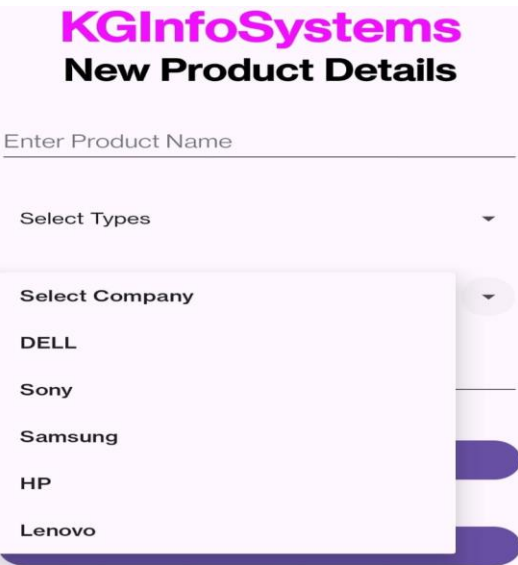
KGInfoSystems
New Product Details

Enter Product Name

Select Types

- Laptop
- Desktop
- Mobile
- Headset
- Charger

Go Back



KGInfoSystems
New Product Details

Enter Product Name

Select Types

Select Company

- DELL
- Sony
- Samsung
- HP
- Lenovo

B11 Figure: Kg info Systems New Product Details

KGInfoSystems
New Property Details

Enter Property Name

Select Types

Enter Property Price

New Property

Go Back

Select Types

- House
- Land
- Building
- Apartment
- Others

B12 Figure: Kg info Systems New Property Details

APPENDIX-C

ENCLOSURES

1. Conference Paper Presented Certificates of all students.











The Project work carried out here is mapped to SDG-3 Good Health and Well-Being.

The project work carried here contributes to the well-being of the human society. This can be used for Analyzing and detecting blood cancer in the early stages so that the required medication can be started early to avoid further consequences which might result in mortality.