IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY APPLICATION USING HAPTIC PIN AND HRNG ALGORITHM FOR ANDROID APPLICATION

Ms. R Annie Karunya, I Vikraman, D.Vivin, R.Pradeep

Faculty, Student, Student, Student
INFORMATION TECHNOLOGY
PSG POLYTECHNIC COLLEGE, COIMBATORE, INDIA

Abstract: Normal PIN section plans are defenseless against perception assaults. Improve the protection from perception assaults, some perception assaults safe PIN-passage plans for mobile phones in light of sounds or potentially hepatics have been proposed. Not with standing, none of existing perception assaults safe PIN-passage plans can accomplish both great security and high convenience Perception assaults safe PIN- passage plot, Loc- Hap PIN, for touch screen gadgets giving restricted hepatic criticism. By utilizing the innovation of confined hepatic criticism, the ease of use and the protection from perception assaults are gotten to the next level. Besides, the client can pick the effectiveness security setting appropriate. A check is finished by sending an OTP to the enrolled number and a security question and answer is been set to recuperate the fail to remember secret phrase. In the event that somebody attempt to get to it will catch the people picture and will ship off the enrolled number.

I. Introduction

The cornerstone of our proposal lies in the utilization of Haptic PIN technology, which leverages the tactile feedback capabilities of smartphones to create a dynamic and intuitive authentication experience. By replacing static numerical inputs with customizable haptic patterns, users can establish highly personalized and inherently secure access codes, significantly reducing the risk of brute-force attacks and unauthorized access.

1.1 OVERVIEW AND ISSUES SOLVED

The infiltration pace of the mixed media savvy phone has persistently expanded. As per the measurements given by Strategy Analytics (SA), an IT statistical surveying institution, the number of the mixed media advanced cell clients at present surpasses 1 billion. However, since the sight and sound PDAs are taken wherever by clients generally due to its helpful elements are liable to be lost or taken. Subsequently, most mixed media PDAs are currently furnished with different underlying locking features

2. Personalized Learning: In the rapidly evolving landscape of digital security, the integration of personalized learning methodologies with cutting-edge technologies has emerged as a cornerstone in fortifying Android application security. This introduction unveils a pioneering fusion of personalized learning principles with Haptic PIN and HRNG (Hardware Random Number Generator) Algorithm, presenting a paradigm shift in how users engage with security measures.

3. Real-World Application: One real-world application for a security application utilizing Haptic PIN and HRNG Algorithm for Android could be in the realm of mobile banking and financial transactions.

4. Accessibility and Inclusivity: Incorporating accessibility and inclusivity features into a security application utilizing Haptic PIN and HRNG Algorithm for Android is essential to ensure that users of all abilities can securely access and protect their sensitive information.

5. Collaboration and Communication: By fostering collaboration and communication throughout the development process, teams can work together effectively to create a secure and user-friendly application that leverages Haptic PIN and HRNG Algorithm for Android.

6. Teacher Training and Professional Development. This proactive approach not only enhances students' cybersecurity awareness but also contributes to building a safer and more secure digital environment.

1.2 PROBLEM DEFINITION

To address these challenges, there is a demand for a security application that leverages innovative technologies such as Haptic PIN and HRNG Algorithm specifically tailored for the Android platform. The primary goal is to provide users with a secure and intuitive authentication experience while mitigating the risk of unauthorized access and data breaches.

1.Inadequate Security Measures: Existing authentication methods in Android applications may not offer sufficient protection against evolving security threats, putting users' sensitive information at risk.

2.Usability and User Engagement: Traditional authentication methods often lack user engagement and customization options, leading to poor user experience and potential security vulnerabilities due to predictable patterns.

3.Need for Innovation: There is a need for innovative security solutions that leverage advanced technologies to enhance security without compromising usability and accessibility.

4.Platform Compatibility: The solution must be compatible with the Android platform, considering the prevalence of Android devices and the need to provide consistent security measures across different devices and versions.

5.Educational Component: There is a need to educate users about the importance of security and how to effectively use the new authentication methods to ensure widespread adoption and compliance.

To develop a security application for Android that incorporates Haptic PIN and HRNG Algorithm to provide users with a secure, customizable, and user-friendly authentication experience.

1.2 PROPOSED SYSTEM

The principle thought behind this application is to improve the security. At first the client register the necessary fields and get the OTP. Haptic criticism framework is accessible to forestall shoulder riding assaults that sends OTP to any enrolled portable GSM device. The Random vibration for the each pin is produced. Assuming somebody attempt to abuse the pin their picture is been catch and shipped off the proprietor's enrolled versatile number. The techniques have utilized for this application are as per the following:
A pseudo-irregular number generator (PRNG) is a program composed for, and utilized in, likelihood and measurements applications when huge amounts of arbitrary digits are required. The greater part of these projects produce vast strings of single- digit numbers, normally in base 10, known as the decimal framework. Whenever enormous examples of pseudo-irregular numbers are taken, every one of the 10 digits in the set {0,1,2,3,4,5,6,7,8,9} happens with equivalent recurrence, despite the fact that they are not equally disseminated in the arrangement.

II. LITERATURE SURVEY

1.**"Enhancing Mobile Application Security Using Haptic PIN Technology**": This paper explores the use of Haptic PIN technology as a novel authentication method for mobile applications

2.**"Hardware Random Number Generators: A Review of Algorithms and Applications":** This review article provides an in-depth analysis of hardware random number generators (HRNG) algorithms and their applications in various domains, including cybersecurity

3.**"Usability and Security of Authentication Methods in Mobile Banking Applications":** This research paper investigates the usability and security implications of different authentication methods, including PINs, passwords, biometrics, and graphical passwords, in mobile banking applications.

4.**"Towards Secure Authentication on Android Devices Using Haptic Feedback":** This study proposes a novel approach to secure authentication on Android devices using Haptic PIN technology

5.**"Integrating Hardware Random Number Generators in Mobile Security Applications**": This article discusses the integration of hardware random number generators (HRNG) in mobile security applications to enhance cryptographic key generation and secure communication

3. Methodology

i. **Determine the purpose of the database** - This helps prepare for the remaining steps.

ii. **Find and organize the information required** - Gather all of the types of information to record inthe database, such as product name and order number.

iii. **Divide the information into tables** - Divide information items into major entities or subjects, suchas Products or Orders. Each subject then becomes a table.

iv. **Turn information items into columns** - Decide what information needs to stored in each table. Each item becomes a field, and is displayed as a column in the table. For example, an Employees table might include fields such as Last Name and Hire Date.

v. **Specify primary keys** - Choose each table’s primary key. The primary key is a column that is used to uniquely identify each row. An example might be Product ID or Order ID.

3.1 CODE DESIGN

The main purpose of code design is to simplify the coding and to achieve betterperformance and quality with free of errors. The coding is prepared in such a way that the internal procedures are more meaningful validation manager is displayed for each column. Thecoding of the variables is done in such a way that one other than person who developed the packages can understand its purpose. To reduce the server load, theproject is designed in a waythat most of the Validation of fields is done as client side validation, which will be more effective.

3.2 DATABASE DESIGN

Database design is the process of producing a detailed data model of a database .This logical data model contains all the needed logical and physical design choices and physical storageparameters needed to generate a design in a Data Definition Language ,which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity. The term database design can be used to describe many different parts of the design of an overall database system. Principally, and most correctly, it can be thought of as the logical design of the base data structures used to store the data.

SYSTEM ANALYSIS

System analysis for Augmented Reality (AR) in education involves evaluating the current educational landscape, identifying System analysis for a security application utilizing Haptic PIN and HRNG Algorithm for Android involves a comprehensive examination of the application's requirements, functionalities, and design considerations to ensure its effectiveness and usability.

Firstly, it entails identifying the specific security needs and objectives of the application, such as protecting sensitive user data, preventing unauthorized access, and complying with industry standards and regulations. This analysis involves assessing potential security threats and vulnerabilities relevant to Android applications and determining the appropriate security measures, including the integration of Haptic PIN and HRNG Algorithm.

Secondly, system analysis involves defining the functionalities and features of the application, including authentication mechanisms, data encryption, secure storage, and user interface design. This requires a thorough understanding of how Haptic PIN technology and HRNG Algorithm will be implemented to provide secure and user-friendly authentication experiences for Android users.

Additionally, system analysis involves evaluating the compatibility and integration of Haptic PIN and HRNG Algorithm with other components of the Android platform, such as the device's hardware, operating system, and security frameworks. This ensures seamless interoperability and optimal performance of the security application on a wide range of Android devices.

SYSTEM DESIGN

I. INPUT DESIGN

Input plan is the method involved with changing over the client arranged Input toa PC based design. The objective of the information configuration is to make the informationsection simpler, coherent and free blunder. Mistakes in the info information are constrained by the information plan. The nature of the info decides the nature of the framework yield.

The whole information section process is intelligent in nature, with the goal that the client can straightforwardly go into information as per incited messages. The clients additionally straight forwardly go into information as indicated by the provoked messages. The clients are likewise given choice of choosing a suitable contribution from a rundown of values.

The quantity to mistake which are generally prone to emerge somehow managed to be placed by the actual client. Input plan is one of the main period of the framework plan. Inputplan is the cycle where the info got in the framework are arranged and planned, to get essentialdata from the client, it isn't expected to kill the data that. The fact that understood by the client

makes The place of the info configuration is to guarantee the most extreme potential degrees of exactness and furthermore guarantees that the information available. The information configuration is the piece of by and large framework plan, which requires exceptionally cautious consideration. In the event that the information going into the framework is mistaken,the handling and result will amplify the blunders.

II. Output Design

The result type of the framework is either by screen. Yield configuration targets producing the after effects of the handling of the clients. The reports are created to suit the requirements of the clients. The reports must be produced with proper levels.. As its web application yield is planned in an extremely easy to use this will be through screen more oftenthan not. The principle motivation behind code configuration is to improve on the coding and to accomplish better execution and quality with liberated from mistakes. The coding is ready so that the inner methodology are more significant approval administrator is shown for every segment.

The coding of the factors is done so that another than individual who fostered the bundles can figure out its motivation. To diminish the server load, the venture is planned in away that the vast majority of the Validation of fields is done as client side approval, which willbe more viable. Data set plan is the most common way of creating a nitty gritty information model of a data set. This sensible information model contains all the required legitimate and actual plan decisions and actual stockpiling boundaries expected to produce a plan in a Data Definition Language, which can then be utilized to make a data set.

A completely credited information model contains point by point ascribes for every substance. The term information base plan can be utilized to portray various pieces of the planof a general data set framework. Essentially, and most accurately, it tends to be considered the coherent plan of the base information structures used to store the information.

IMPLEMENTATION AND TESTING

IMPLEMENTATION

In existence without the proper usage of security or locks in Mobile Phones which leads to vulnerability of stealing others personal information. This personal information involves misusing others photo's, banking details, getting some important documents being misused by others without proper security scheme. The problem of security is growing very bad due to smart phone usage.This project is a mobile application based project to enhance security. "PIN SECURITY SCHEME USING HAPTIC FEEDBACK" is a user-friendly software application. The purpose ofthis project is to provide a better security, a software solution that delivers a scalable, secure,and reliable application that maintains and manages the application details. The feature of the"PIN SECURITY SCHEME USING HAPTIC FEEDBACK" and the requirements that the project will adhere to developing the software for the user security purpose.

Testing is the most important phase in the software development activity. Insoftware development life cycle (SDLC), the main aim of the testing process is the quality the developed software is tested against attaining the required functionality and performance. During the testing process the software is worked with some particular testcase and the output of the test cases are analyzed whether the software working according to the expectations or not.The success of the testing process in determining the error is mostly depends up on thetestcase criteria, for testing any software need to have a description of the expected behaviour of the system and method of determining whether the observed behaviorconfirmed to the expected behavior . Requirement testing is one of the kind where testing isdone before the commencement of the project. Before commencing the project, requirements listed out by the client are checked for its feasibility.

SYSTEM TESTING:

Haptic PIN Setup Testing: Verify that users can successfully set up their Haptic PIN patterns and associate tactile feedback with PIN digits. Test various combinations of patterns to ensure usability and accessibility for users with diverse needs and preferences.

Authentication Testing: Test the authentication process to ensure that users can successfully log in using their Haptic PIN. Verify that the system accurately verifies user input and grants access upon successful authentication. Test for scenarios such as incorrect PIN entries, device lockouts, and recovery procedures.

HRNG Algorithm Testing: Validate the functionality of the HRNG Algorithm in generating random cryptographic keys used for securing sensitive data. Test the unpredictability and integrity of generated keys under various conditions to ensure robustness and reliability.

Data Encryption and Decryption Testing: Test the encryption and decryption processes to ensure the security and integrity of sensitive user data stored locally on the device and transmitted over networks. Verify that encrypted data remains protected and that decryption operations yield accurate results.

Usability and Accessibility Testing: Conduct usability and accessibility testing to ensure that the application meets the needs of users with diverse abilities and preferences. Test for factors such as interface clarity, navigation ease, and compatibility with accessibility features such as screen readers and alternative input methods.

Performance Testing: Evaluate the performance of the application under various load conditions to ensure responsiveness and efficiency. Test for factors such as login speed, data encryption/decryption latency, and resource utilization to identify and address potential performance bottlenecks.

Security Testing: Conduct security testing to identify and mitigate potential vulnerabilities and threats. Test for common security issues such as brute-force attacks, data interception, and unauthorized access attempts. Verify that the application adheres to industry standards and best practices for security.

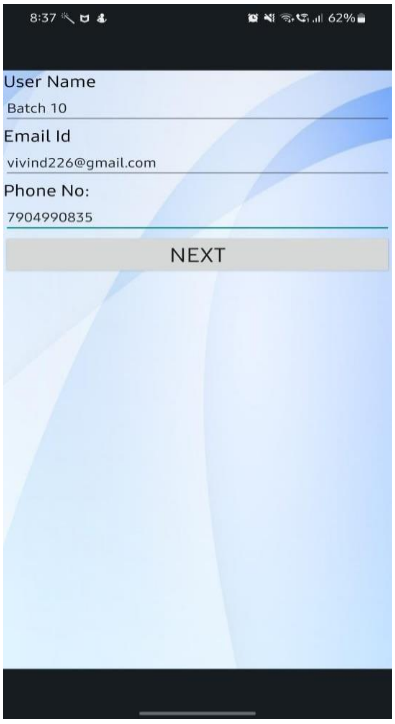
Integration Testing: Test the integration of various components within the application, including the Haptic PIN authentication module, HRNG Algorithm, user interface elements, and backend systems. Verify that all components work together seamlessly to provide a cohesive and reliable security solution.

FUTURE ENHANCEMENT

The project PIN security scheme using Haptic feedback is very simple in design and to implement. The mobile requires very low resources and works in almost all configurationsand its interface is very user-friendly. It include registration of the user, then the random vibrations are counted which is added with already existing PIN and new password is generated every time. The generated new password is been typed to unlock an app.

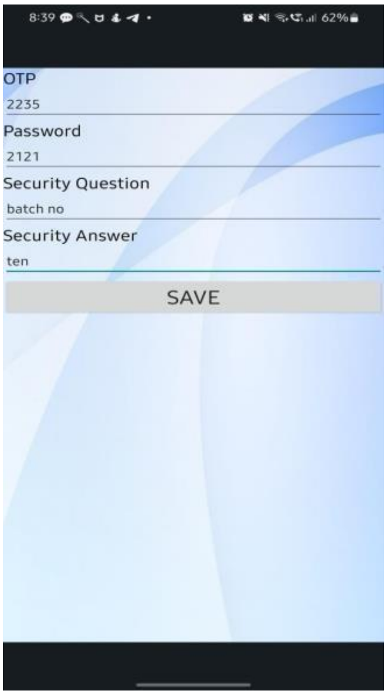
Same Mobile application can be developed for others Mobile operating systems suchas Windows, iOS etc. Existing software is developed for Mobile phones of Android operatingsystem with lollipop version and below. Same application can be developed for higher android version. In current project, have added security only for the calculator application. In future,the user could able to select any applications available in mobile phone selected applications can be secured.

PROJECT OUTPUTS:



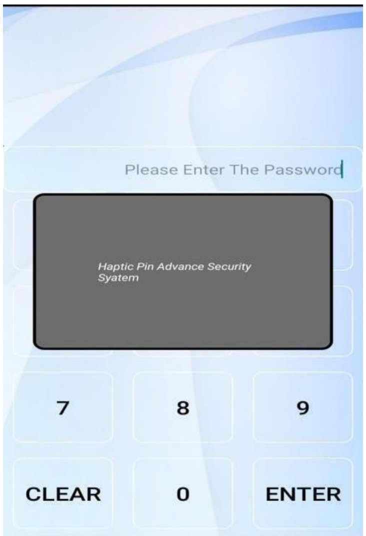
User Name
Batch 10
Email Id
vivind226@gmail.com
Phone No:
7904990835

FIG.1.1 Registration Page



OTP
2235
Password
2121
Security Question
batch no
Security Answer
ten

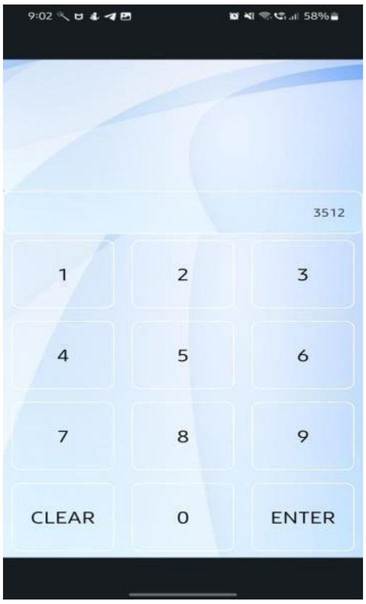
FIG.1.2 OTP and PIN
setting



Please Enter The Password

Haptic Pin Advance Security Syatem

FIG.1.3 4 Lock Screen and Vibration on Device



3512

FIG.1.5 PIN ENTERING AND VALUE CHECK

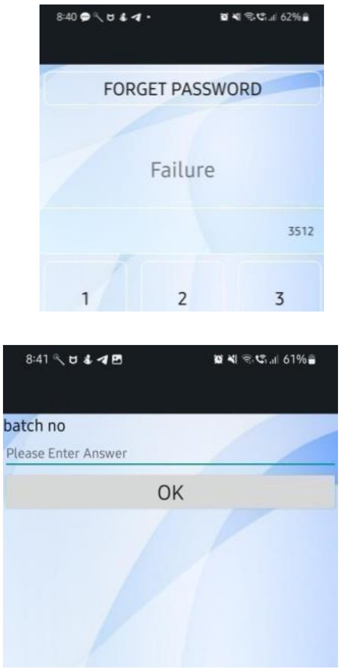


FIG.1.6 Forget PIN and Security question

References

[1] EE Delhi Section Conference (DELCON)YEAR:2022

[2] Identification of Possibly Intemperate Permission Demands in Android Apps Pradeep KumAssessment on Impact of Social-Media on Teenagers,Jyoti Singh;Manju 2022 IEar Tiwari;Srinivasa Reddy Basireddy;Velayutham T 2022 2nd ICIPTM,Year: 2022

[3] A Comparative Analysis of SMS Spam Detection employing Machine Learning Methods 2022 6th ICCMC ,Year: 2022

[4] SoundID: Securing Mobile Two-Factor Authentication via Acoustic Signals Dan Liu;Qian Wang;Man Zhou;Peipei Jiang;Qi Li;Chao Shen;Cong Wang IEEE Transactions on Dependable and Secure Computing,Year: 2022

[5] A Systematic Study of Android Non-SDK (Hidden) Service API Yi He;Yacong Gu;Purui Su;Kun Sun;Yajin Zhou;Zhi Wang;Qi Li IEEE Transactions on Dependableand Secure ComputingYear: 2022