International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Project Authentica

[1]Mr. Harsh Solanki, [2]Miss. Neha Shaikh, [3]Mr. Kellen Massey, [4]Mr. Vaibhav Mestry, [5]Miss. Aishwarya Manjalkar

[1]Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.
[2]Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.
[3]Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.
[4]Department of Information Technology, Pravin Patil Polytechnic, College of Engineering, Bhayander, Thane, India - 401105.
[5]Professor of Pravin Patil Polytechnic, Department of Information Technology, Bhayander, Thane, India - 401105.

ABSTRACT- —

Authentication is process of validating the user 's identity. Users are identified using different authentication mechanisms. In a security system the authentication process checks the information provided by the user with the database. If the information matches with the database information, the user is granted access to the security system The authentication system is one of the most important methods for maintaining information security in smart devices. There are many authentication methods, such as password authentication, biometric authentication, signature authentication, and so on, to protect cloud users' data. However, online information is not yet effectively authenticated method. Our main motive is to create such a platform or application which is genuine and trustworthy for the users. Looking towards crypto and nfts community there is always a risk of being hacked or getting scammed to overcome with this situation our application is very useful for them as it will provide security, protectivity and privacy as well.as we all experienced it on our daily basis that social media is very beneficial but is also harmful in the same way because of the scamps and cyberpunk, we assure our users with complete secrecy ,privacy, genuine and a trustworthy platform.

INTRODUCTION

Project Authentica a is a social media platform specifically designed for crypto and nft's community.in today's generation of social media, there is a problem arising of fake/bot accounts.so, the solution to the problem can be solved through this project Authentica. Project authentica will follow static and dynamic procedure to eliminate bot accounts with strict verification. This project will helps us to build a social media platform with the genuine users there will be no fraud which will make this platform more secure for the genuine users.

Authentication is a process of verifying a user or device before allowing access to a system or resources.in other words, authentication means confirming that a user is who they say they are. This ensures only those with authorized credentials gain access to secure systems.

Authentication factors can be classified into three groups: -

- A password or personal identification number
- Something you have token based.
- Biometrics, such as fingerprints or face recognition.
- Benefits for implementing authentication to the social media platforms: -
- To control access to a system or application. To bind some sensitive data to an individual, such as for encryption.
- To establish trust between multiple parties to form some interaction with them.
- To assure that a piece of information is genuine.
- To give or provide security and privacy to the user.

LITERATURE SURVEY

To better enforce security in online services, authentication has been the major means of defense. Itis considered as the primary line of protection that plays a crucial role to verify and Validate the authenticity of a user before gaining access to protected system or allowing online transactions. Various authentication schemes-based token-based, and biometric-based few articles were reviewed, evaluated, and analyzed after the eligibility process in this study. The search was thoroughly done according to the objective of this review, which is to study the current types of authentication methods as safe practice for information security among Internet users. The studies were classified into relevant themes by using qualitative synthesis. This was done by reading the title, abstract, and keywords of each study. Furthermore, a thematic analysis was performed to classify themes related to type of authentication method. Through an article review process relevant groups were identified. Finally, a total of three main themes including password authentication, biometric authentication, and multifactor authentication methods emerged. Password-based methods were grouped into textual and graphical authentication. Biometric methods were classified into fingerprint, facial, retina or iris, voice, and digital signature authentication. Several review processes were done by the authors to finalize the themes and sub-themes.

- Password authentication Password has been used to protect online information since the early existence of the Internet. Passwords often do not expire, and users tend to use the same password for a long period, which leads to cyberattacks [53]. Passwords are one of the most significant risk factors because they are vulnerable to threats and attacks. Thus, a well- formulated and structured password should be “easy to remember but hard to hack”. In this paper, the review has found two sub- themes under password authentication: textual and graphical.
- Biometric authentication the security of biometric identification depends on body patterns such as fingerprints or facial features. This type of authentication has the uniqueness derived from a human body. Biometric authentication has been increasingly used as it provides a more secured process of identifying users. Biometric authentication methods are more likely to be convenient, secure, and strong used compared with traditional authentication methods. This section discusses fingerprint,facial feature, retina/iris, voice, and digital signature authentication.

SYSTEM OVERVIEW

An authentication application for Android typically involves several components that work together to provide secure and reliable user authentication. Here is an overview of the major components that may beinvolved:

User Interface: This component provides the graphical user interface (GUI) for the authentication application. The user interface allows the user to enter their credentials (e.g., username and password) and initiate the authentication process.

Authentication Backend: This component performs the actual authentication of the user. It typically communicates with the server-side authentication system (e.g., LDAP, Active Directory, OAuth) to verify the user's credentialsand obtain an access token or other form of authentication token.

Security Measures: This component ensures the securityand integrity of the authentication process. It may involve using encryption algorithms for password storage, implementing multi-factor authentication (e.g., biometric authentication, one-time passwords).

Error Handling and Logging: This component handles errors that may occur during the authentication process and logs relevant information for debugging and analysis. Integration with Other Applications: This component may involve integrating the authentication application with other applications and services, such as email clients or social media platforms, to enable seamless authentication across different platforms.

Compatibility with Android Devices: This component ensures that the authentication application is compatible with various Android devices and operating system versions, and that it meets the relevant security standards and guidelines.

User Management: This component manages user accounts and permissions, including creating new user accounts, modifying existing accounts, and revoking access as needed.

Overall, the key goal of an authentication application for Android is to provide a secure, reliable, and user-friendly authentication experience for users, while also meeting the relevant security standards and guidelines.

METHODOLOGY

Plan and define the authentication flow: You should start by defining the authentication flow of your app. What type of authentication will you be using (e.g., email and password, social media login, biometrics)? What screens will be involved in the authentication process?

Set up a new Android Studio project: Open Android Open Android Studio and create a new project. Select "Empty Activity" as the template.

Design the user interface: Using the XML layout files, design the user interface for your app. This should include the screens involved in the authentication process, such as the login screen, registration screen, and password reset screen.

Implement authentication logic: Write the Java code to implement the authentication logic for yourapp. This will involve validating user input, checking user credentials, and handling authentication errors.

Integrate with a backend server: If your app requires communication with a backend server for authentication purposes, you will need to integrate your app with the server. This can be done using APIs or other protocols.

Test and debug: Test your app on a variety of devices and Android versions to ensure that it works correctly. Debug any issues that you encounter. Studio and create a new project. Select "Empty Activity" as the template.

SODTWARE DISCRIPTION

Design the user interface: Using the XML layout files, design the user interface for your app. This should include the screens involved in the authentication process, such as the login screen, registration screen, and password reset screen.

Publish your app: Once your app is complete, publish it to the Google Play Store or other app stores.

Some best practices to keep in mind while developing an authentication app include:

Use secure protocols and encryption methods to protect user data. Provide clear feedback to users about the authentication process and any errors that occur. Use best practices for storing and managing user credentials (e.g., salted, and hashed passwords) Use secure and unique session tokens to manage user sessions.

Regularly test and update your app to address security vulnerabilities.

Use secure and unique session tokens to manage user sessions Regularly test and update your app to address security vulnerabilities.

Together, Android Studio and Firebase provide a powerful platform for developers to create high- quality, feature-rich, and scalable mobile applications for Android. Developers can use Android Studio to write code and build the user interface of their app, while Firebase provides backend services such as cloud storage, authentication, and database management to help developers build, improve and grow their applications. The integration of Android Studio and Firebase makes it easy for developers to create and deploy high-quality Android applications quickly and efficiently.

SDK-

SDK stands for Software Development Kit. It is a set of software development tools that enable developers to create applications for a specific platform or operating system. An SDK typically includes libraries, APIs (Application Programming Interfaces), documentation, and other tools needed for developing software applications.

SDKs are used by developers to build applications for different platforms such as desktop computers, mobile devices, game consoles, and web applications. SDKs can be specific to a particular operating system or platform such as iOS, Android, Windows, or Linux.

An SDK typically includes the following components: Libraries - pre-built code modules that developers can useto perform specific tasks such as networking, graphics, audio, or user interface.

APIs - Application Programming Interfaces that define how developers can interact with the platform's features and functions.

Tools - software tools that help developers build, test, and deploy applications.

Documentation - comprehensive documentation that explains how to use the SDK and its components.

Sample code - pre-built code examples that demonstrate how to use the SDK's components to build a working application.

Overall, an SDK is an essential tool for developers who want to create applications for a specific platform or operating system. It provides a standardized way for developers to access the platform's features and functions, reducing development time and complexity.

TensorFlow lite-

TensorFlow Lite is a software library developed by Googlethat allows developers to deploy machine learning models on mobile and embedded devices. It is a lightweight version of the TensorFlow machine learning framework, designed specifically for use on mobile devices with limited computational resources.

TensorFlow Lite offers a range of features that make it easy for developers to deploy machine learning models on mobile and embedded devices. Some of these features include:

Fast performance - TensorFlow Lite is optimized for mobile and embedded devices, and it can run machine learning models quickly and efficiently, even on devices with limited processing power.

Small footprint - TensorFlow Lite is designed to have a small footprint, making it easy to deploy on mobile devices with limited storage capacity.

Easy integration - TensorFlow Lite can be easily integrated into existing mobile and embedded applications, allowing developers to add machine learning capabilities to their applications quickly andeasily.

Compatibility - TensorFlow Lite is compatible with a wide range of mobile and embedded devices, includingAndroid and iOS devices, Raspberry Pi, and microcontrollers.

Flexibility - TensorFlow Lite supports a wide range of machine learning models, including custom models created by developers, making it a flexible platform platform for building intelligent applications for mobile and embedded devices.

This metric measures how well the application can accurately identify and verify the user's identity. The accuracy can be measured by comparing the application's results to the actual identity of the user.

Security: Authentication applications need to be secure to protect user data from potential breaches. Therefore, it is essential to evaluate the application's security features, including encryption, two-factor authentication, and other measures.

User experience: A good authentication application should be easy to use and navigate. The application should have a simple and intuitive interface that allows users to quickly and easily authenticate themselves.

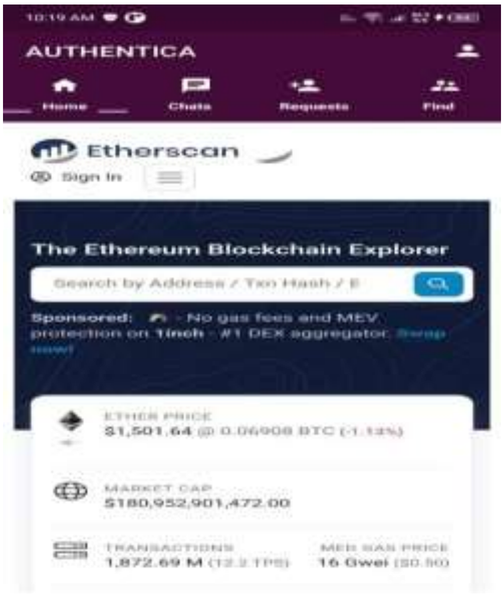
Integration: Integration with other applications and systems is also crucial. The application should be able to integrate with other systems seamlessly, such as enterprise systems or mobile applications.

Cost: Finally, the cost of the application is also a critical factor. Organizations need to evaluate the total cost of ownership, including licensing, deployment, and maintenance costs.

Overall, a successful authentication application should have high accuracy, strong security features, a good user experience, seamless integration, and reasonable costs. Organizations can evaluate these factors to determine which authentication application best fits their needs.

For machine learning on mobile and embedded devices.

Overall, TensorFlow Lite is an excellent choice for developers who want to deploy machine learning models on mobile and embedded devices. It offers fast performance, a small footprint, and easy integration, making it an ideal



The Ethereum Blockchain Explorer

Search by Address / Txn Hash / B

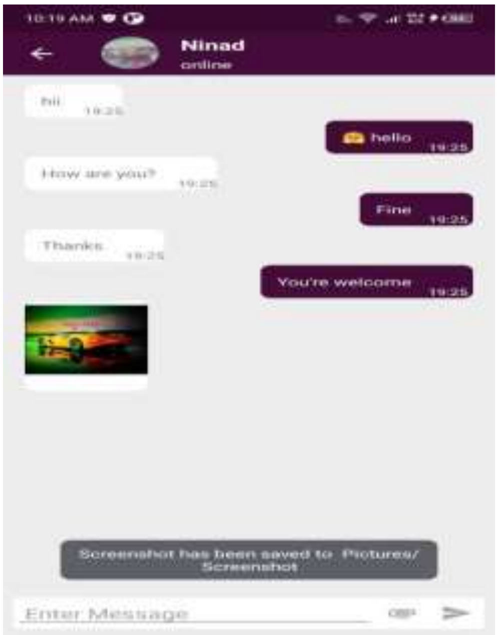
Sponsored: - No gas fees and MEV protection on 1inch - #1 DEX aggregator. Swap now!

ETHER PRICE
$1,501.64 @ 0.06908 BTC (-1.13%)

MARKET CAP
$180,952,901,472.00

TRANSACTIONS
1,872.69 M (12.2 TPS)

MED GAS PRICE
16 Gwei ($0.50)



hii 19:25

hello 19:25

How are you? 19:25

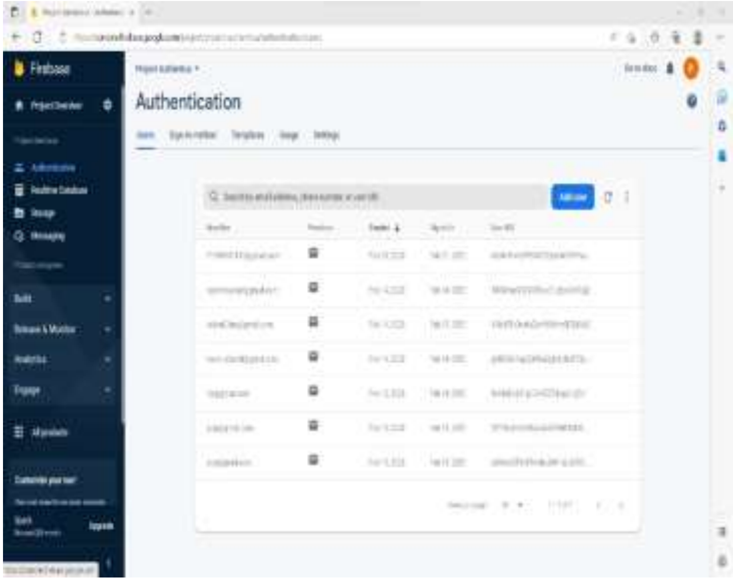
Fine 19:25

Thanks 19:25

You're welcome 19:25

Screenshot has been saved to Pictures/Screenshot

Enter Message



Authentication

CONCLUSION

This can be a booming platform in crypto worldfor crypto community..

FUTURE SCOPE

- This can be booming platform in crypto world for crypto.
- This platform is beneficial for genuine users.
- It will be one of the trustworthy platform.

REFERENCES

1) google.com