# ENHANCING AUTHENTICATION MEASURES AND USER AUTHENTICITY ON META PLATFORMS

MSc Research Project
Cybersecurity

Shubham Gupta
Student ID: 22186018

School of Computing
National College of Ireland

Supervisor: Mr. Jawad Salahuddin

**National College of Ireland**

**MSc Project Submission Sheet**

**School of Computing**

**Student Name:** Shubham Gupta……………………………………………………………………………………

**Student ID:** 22186018……………………………………………………………………………………..……

**Programme:** MSc Cybersecurity………………………………………… **Year:** 2023-2024…..

**Module:** MSc Research Practicum……………………………………………………………….………

**Supervisor:** Mr. Jawad Salahuddin…………………………………………………………………….………

**Submission Due Date:** August 12, 2024………………………………………………………………………….………

**Project Title:** ENHANCING AUTHENTICATION MEASURES AND USER AUTHENTICITY ON META PLATFORMS……………………………………………………………………….………

**Word Count:** 5410…………………………… **Page Count:** 14……………………………………………..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

**Signature:** Shubham Gupta………………………………………………………………………

**Date:** August 11, 2024…………………..………………………………………………………

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

| | |
|---|---|
| Attach a completed copy of this sheet to each project (including multiple copies) | □ |
| **Attach a Moodle submission receipt of the online project submission,** to each project (including multiple copies). | □ |
| **You must ensure that you retain a HARD COPY of the project**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | □ |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| **Office Use Only** | |
|---|---|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

# ENHANCING AUTHENTICATION MEASURES AND USER AUTHENTICITY ON META PLATFORMS

Shubham Gupta
22186018

## Abstract

This research explores the vulnerabilities aligned with user authentication system on Meta platforms which is currently allowing to create fake accounts using different attack vectors such as identity fraud and SIM swapping. This raises concern for strengthening user validation on Meta platforms which can mitigate fake accounts and enhance traceability of users for digital forensics. To address these issues, a multi-layered solution is proposed that uses Auth0, React libraries, and Node.js for authenticating users with legitimate national ID information. The method considers learnings from other researchers work which helps to create a strong user validation system. Additionally, another authentication system is placed using the same prototype and infrastructure to verify login attempts made using push notification mechanism which ensures that only legitimate user can gain access. The complete solution bounds the virtual identity of an individual with their verified physical identities which enhances the traceability of users for cyber-criminal investigations, However, research work also highlights challenges faced such as global applicability and potential privacy concerns when handling crucial private information. By addressing the marked challenges, research work also offers future solutions such as assigning of unified identity number and sharing digital wallet identity number. The research work presents a secure approach to improve user authenticity on Meta platforms for a secure online environment for any individual.

# I. INTRODUCTION

Meta Platforms Inc., which earlier known as Facebook Inc., has made a name for itself in the field of digital communication and social media. Meta acquired almost half of the global population as an estimated 3.98 billion active users each month. This strong user base is spread across multiple platforms offered under the umbrella of Meta such as Facebook, WhatsApp, and Instagram. The large chunk of active users is acquired under Facebook which is 3.07 billion and remaining 0.91 billion users is spread among other Meta platforms.

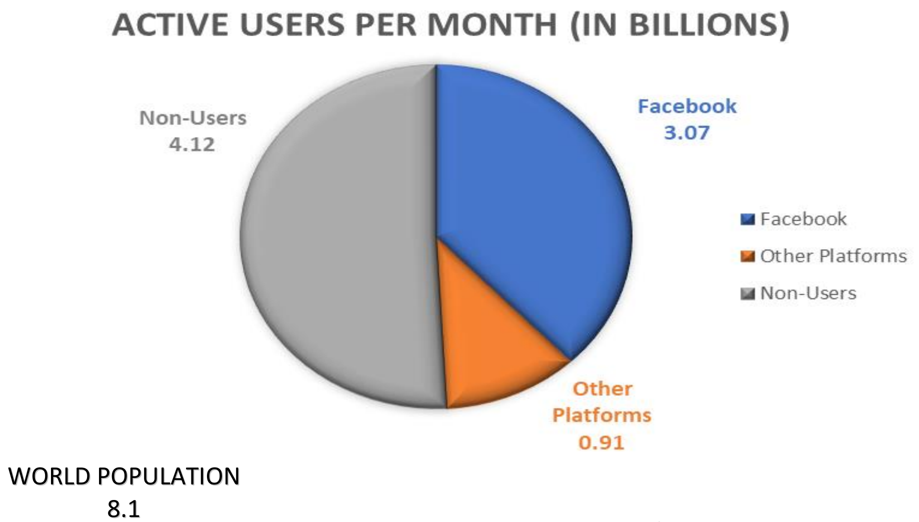


**Figure I. Meta User Base Compared to World's Population**

Nevertheless, there are various issues which pose with this large user base, specially when it comes to the authenticity of the users and authentication measures put in place to stop the creation of fake accounts and spoofing identities. This research focuses on highlighting the problem related to user authentication and propose improved techniques to guarantee the validity and integrity of user identities on Meta platforms.

## I.I. BACKGROUND

Meta platforms are becoming essential for everyday tasks such as social contact, corporate operations, and communication channels for billions of people which showcase Meta's global reach. The size of the company's user base mentioned in financial filings with Securities and Exchange Commission (SEC) justifies success and the confidence of customers in their platforms. (Meta, 2024)

However, this large user base brings significant challenges particularly in terms of ensuring the legitimacy and authenticity of users. Also, presence of fake accounts and identity fraud hampers user trust on the longer run.

### I.I.I AUTHENTICATION MECHANISM

Currently, Meta relies on third-party platforms and services such as email providers and telecommunications companies, to authenticate users. These telecommunication providers plays an important role as they perform various checks to provide a phone number to an individual including validation of identity proofs such as driving license, national ID proofs or biometric scans such as fingerprint, facial recognition. When the user receives a valid phone number, user can use it along with email address provided by the email providers during the account creation phase of Facebook.

This complete multi-layered process seems secure and trustworthy which ensures that only legitimate users can access Meta's environment and connect globally. However, this complete process have its own flaws and vulnerabilities which needs to be fixed.

### I.I.II SECURITY CONCERN

The above-mentioned authentication frameworks looks well-built but it have two main security risks which are SIM swapping / switching and Identity fraud. Identity fraud is the illegal use of any individual's personal information which can help fraudsters to gather SIM cards or can open fake social-media accounts which can hamper victim's reputation. Another method where attackers can get control of user's phone in order to forward One Time Passwords (OTPs) obtained in the form of Short Message Service (SMS) or can physically change SIM cards. Both the techniques can be classified as SIM swapping or SIM hijacking.

This allows the attackers to get SMS-based authentication done to create fake accounts under the use of legitimate channels. These frauds raise concerns about the security of Meta platforms and their user base, hence Meta requires to implement strong security measures in order to mitigate the current security risks.

## I.II Problem Discussion

### I.II.I Legitimacy Of User Account

Security measures of Meta platforms has become a major concern as their business model mostly depends on connecting with legitimate users which directly aligns with consumer trust. A number of threats such as distribution of false information, financial fraud, and compromise of user privacy can posed by spoofed or fake accounts. These spoof accounts can ruin the overall user experience and can affect the platform's potential and efficiency.

Furthermore, these fraudulent accounts can be used for illegal and criminal activities such as spamming, launching phishing attacks, and more. Though, Meta have a complex verification process, there are still loopholes that can be exploited by cyber criminals in order to generate fake profiles which look just like the original ones. This severely compromises the integrity of the platform and reduces user trust.

### I.II.II Identity Fraud

Identity fraud is an important issue which requires attention as it bring serious risk for both, users and platforms. Attackers can take leverage of stolen or spoofed identities in order to bypass the verification process of respective platforms that helps them to create fake accounts. This can be achieved by availing the personal information through data breaches, social engineering and phishing attacks. Once the attacker have the personal information associated with the targeted account, they can take over accounts or can create a replica of the original account by using false identities. Identity theft can result in financial losses, harm to individual's reputation, and weakens user trust while communicating on the platform.

### I.II.III SIM Swapping

SIM swapping is another important threat to user security which particularly affect the effectiveness of two-factor authentication (2FA) mechanisms. Scammers can convince telecommunication providers to transfer a user's SIM card to a new SIM card or can conduct a social engineering attack convincing the user to forward SMS to another number using numpad shortcut keys. Once the attacker have the control of the victim's phone number, they can receive SMS-based authentication codes which effectively bypass 2FA and help gaining access to different types of accounts such as social-media, banking, and more.

SIM swapping use vulnerabilities in the verification processes of telecom provider such as insufficient checks made while switching SIM cards between different phones. It left victim with no notification on any channel if attacker uses the clone SIM card on another device. This can have serious repercussions as this gives hackers to complete access to accounts and personal data.

# II. Literature Review

The literature review highlight the challenges associated with user authentication, risk of fake accounts, SIM swapping, and identity fraud. It covers the research papers which are relevant with the research to understand user behaviour and preferences regarding Meta's current security measures. Also, researchers proposed solutions for the identified gaps are also considered to know how they enhanced user trust and platform security. Below-mentioned research papers also provide comments on their strength and weakness:

## II.I FOCUS: IDENTITY FRAUD AND SIM SWAPPING

**1) SIM SWAPPING ATTACKS FOR DIGITAL IDENTITY THEFT** (Hallman, 2023): The research conducted by Roger is directly relevant to the current work as he investigated on SIM swapping and highlighted vulnerabilities aligned with telecommunication infrastructure, both poses a major threat to Meta's user authentication process. Based on identified risks, Roger provided practical solutions such as implementation of hardware token Multi Factor Authentication (MFA) and AI-based behavioral analysis.

While Roger proposed strong solutions that were mainly associated with SIM swapping but his research requires further consideration on other forms of identity fraud. Further, implementation and user adaptation of hardware token MFA requires additional investigation.

**2) INFLUENCER FRAUD ON INSTAGRAM** (Schröder, 2019): The analysis conducted by Jonas that how frequently people are creating fake accounts and their impact directly aligns with current research identified challenge of Meta's maintaining user legitimacy. This research paper focuses on improving user authentication to mitigate fake accounts. He also highlighted that how fake accounts can impact the overall user experience and can raise questions about the platform integrity.

The paper provided a strong analysis but requires specific implementation strategies as it offers a wider view rather than providing a detailed solution. This limits the thought of implementing it into Meta's environment.

**3) THE NEED OF TWO-FACTOR AUTHENTICATION IN SOCIAL MEDIA** (Ikhalia, 2013): Researcher emphasised on 2FA which can also be applied for enhancing Meta's user verification process to mitigate identity fraud and fake accounts. This research proposed an email based password tokenization system which acts as an additional layer of verification to mitigate phishing attacks.

The research work lacks on the connectivity of email address with the physical identity of a user which rises concern with the overall integrity of the system.

**4) THREATS AND PROTECTION ON e-SIM** (Mathew, 2020): Alex did the research in advance technologies such as e-SIM and AI-based advanced fraud detection which can be used as a solution when dealing with e-SIM verification for Meta platforms. Researcher suggests that instead of using the traditional SIM cards, users should opt for embedded e-SIMs as there is no physical presence which mitigates the chances of attacks such as SIM swapping.

The research still needs some work to be done as all the devices are not compatible with e-SIMs and challenges posed by user in accepting this technology is not properly addressed.

## II.II UNDERSTANDING CHALLENGES POSED BY FAKE ACCOUNTS

**1) TEENS, SOCIAL MEDIA, AND PRIVACY** (Mary Madden, 2013)**:** Researchers analysed the trends among teens about the use of social-media platforms and how these platforms encourage them to share a wide portion of their information to be available in public. However, these platforms provide different privacy controls to whom the user can share the information with, but few teens opt for a fully public approach on social media. According to below provided graph, his study marked the increase in the frequency of teenagers sharing information on Facebook in short span of time.

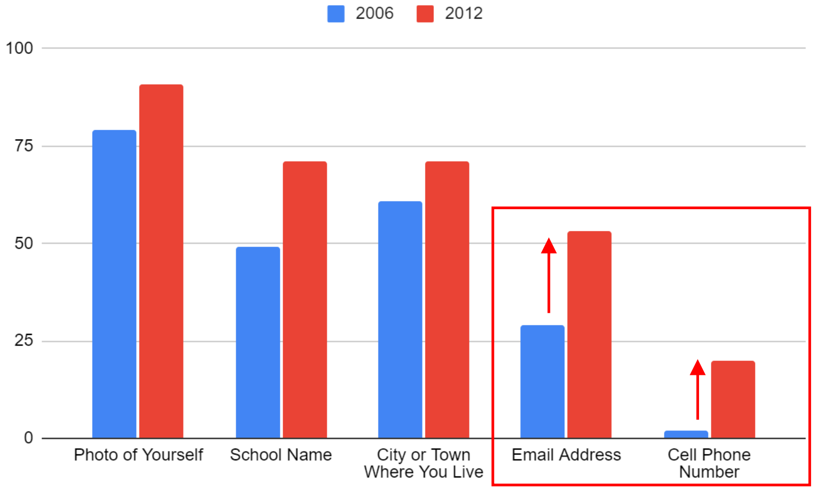


**Figure II. Increase in Data Shared Publicly by Teens on Facebook**

Facebook was introduced in the year 2004 and the considered data is for the year between 2006 and 2012. The analysis highlights that in only few years, likeliness of the platform among diversified communities got increased which encourages individuals to make their identities available in public in terms by sharing their personal information.

**2) HOW DOES FACEBOOK MEASURE FAKE ACCOUNTS?** (Meta, 2019)**:** Meta itself analysed it database for fake accounts which helps them to increase user satisfaction and trust. To achieve this, Meta uses various techniques such as detection of n number of accounts created from one location, number of attempts to login an account, blocking IP ranges, analysis malicious behavior on basis of email addresses and suspicious actions, and removing of already created accounts when reported by other users.

Though, Meta have their own security measures in place still there is a need for more enhanced preventive security measures to mitigate fake accounts completely.

**3) UNDERSTANDING THE PHENOMENON AND RISKS OF IDENTITY THEFT AND FRAUD ON SOCIAL MEDIA** (Ahmad Rafi Ilzan, 2023)**:** The marked study examined the effects of identity fraud and focuses on the criticality of the improved user authentication measures requires on social media sites. According to researcher's analysis, most affected age from these platforms is 22 as maximum number of identity theft complaints got logged with Federal Trade Commission in 2022.

However, the impact of security measures provided by the team is limited as they were focusing on different aspects rather than providing a single solution.

**4) FACEBOOK: DETECTING FAKE PROFILES IN ON-LINE SOCIAL NETWORKS** (Mauro Conti, 2012)**:** The team provided a detailed examination on detection of fake profile methods which provides helpful insights in developing of effective detection strateges of fake accounts. Researchers used machine learining algorithms to train the models on basis of number of OSN friends, real social interaction, and over time strcuture of OSN graph.

Though the proposed solution offers significant improvement with great results but the solution is considered as a corrective measure not a preventive measure. This means, it is allowing users to create a fake accounts.

**5) DETECTING SOCIAL NETWORK PROFILE CLONING** (Georgios Kontaxis, 2014)**:** The paper marks the use of SybilRank algorithm which is a practical tool for detecting fake accounts and it directly aligns with motive of improving user authentication system on Meta platforms. The research showcased high accuracy with the use of algorithm in detecting fake accounts.

Still, the analysis requires further investigation and validation as different platforms have theit own significance on operating the user database.

**6) PROFILING FAKE NEWS SPREADERS ON SOCIAL MEDIA THROUGH PSYCHOLOGICAL AND MOTIVATIONAL FACTORS** (Mansooreh Karami, 2021)**:** Researchers analysed the psychological tactics used by fraudsters which provides an understanding of user behaviour that can be helpful in creating strategies for the detection of fake accounts. They provides a unique perspective which can be helpful to create a solution with effective detection and prevention strategies.

But, research is somewhat more theoritical with less implementation strategies and security measures which can only be considered as to carry forward study on certain grounds.

**7) BLOCKCHAIN TECHNOLOGY FOR AUTHENTICATION AND VALIDATION SOCIAL NETWORK ACCOUNTS** (Zacky Althero, 2023)**:** The team proposed a solution where they were using blockchain techniques on the user personal information which will be stored in individual blocks to be used at time of verification and authentication. So, this appproach provides a single hash to an individual which further mitigates the chances of a single user creating multiple and fake accounts.

However, the research lacks in checking the feasbility of integrating the solution with different infrasturcture which poses practical challeneges.

**8) WHY FAKE SOCIAL MEDIA ACCOUNTS ARE A THREAT TO BUSINESSES TODAY** (Baruchin, 2024)**:** The researcher provides an analysis of fake accounts on social media platforms highlighting the need for appropriate user authentication methods on social media sites. The work also provide evidences on the scale of the problem when the fake accounts be reflected in the platforms database which showcase the requirement of strong security measures.

The marked analysis provides impact in the form of general reccommendations on when the correct security measures are in place but the report doesn’t provides any specific practical information.

**9) Linguistic-Based Detection of Fake News in Social Media** (Mohammad Mahyoob, 2021)**:** The paper tends to provide a solution where it can differentiate between fake and authentic news using linguistic indicators. The researcher used methodological approach which provides insights on the detection techniques that was supported with both qualitative and quantitative data analysis as the team compares 16 attibutes under 3 main linguistic features categories (lexical, grammatical, and syntactic features).

Still, the research needs some more analysis to be done as the attributes selected may not comply with every social-media platform specially with Meta as they comply with user communication not provides a common channel that spreads news among people.

**10) Fake Profile Detection Using Machine Learning Techniques** (Partha Chakraborty, 2022)**:** The study examined the use of machine learning techniques to detect fake accounts which can help in enhancing Meta's detection capabilites of fake accounts. Researchers used models such as LSTM, XG Boost, Random Forest, and Neural Networks which provided advance solutions for detection with impactful results.

The study proposed a highly technical solution which provides practical implementation details including hyperparameters and architecture. But due to the solutions's complex architecture, it can be challenging to implement in Meta's environement.

# III. Methodology

This research focuses on providing a comprehensive framework which evaluates and enhances the user authentication process on the Meta platforms. This analysis particularly address issues of identity fraud and SIM swapping which are leveraged by fraudsters to create fake accounts.

## III.I Research Design

The research followed a mixed approach by combining both qualitative and quantitative techniques to gather information from public sources and to analyse the collected data. The process involves the following steps:

**1) Keyword Search:** Particular keywords are searched such as "SIM swapping / switching attacks", "Identity fraud on social media", "Creation of fake accounts on Meta Platforms", "Ease of creating a fake Gmail account", "Latest authentication measures", and "Auth0 by Okta" with the aim of finding relevant research papers which can support the current work.

**2) Selection Criteria:** All the information is selected based on its relevancy to issues marked in the report such as user authentication, SIM swapping, and identity fraud on Meta platforms.

**3) Cross-Referencing:** The collected information from various different public sources are inter-checked in order to validate the information and also to identify latest practices.

**4) Industry Reports:** Thoughroly analysed industry reports are considered and collected to gain knowledge on the statistical aspects of the study.

**5) Technical Forums:** Differnent community opinions and inputs are gathered which are available on Reddit, Quora, Neowin, Meta, and many other forums to understand and gain knowledge from professionals about different techniques regarding the research work.

## III.II Scenario Analysis

The analysis of Meta's Facebook authentication mechanism has been conducted in order to identify that how easy is the process of creating a fake account on Facebook. The below-mentioned details provide the method to create a fake account:

**1) Gmail Account:** Facebook requires an email address as an identity to a user under which all the details will get stored. This email address will be provided by an email service provider and this study opted for Gmail.

To create a fake Gmail account, Initially Gmail requires First and Last Name followed by Date Of Birth (DOB) and Gender. This should be filled with fake or spoofed details and try providing as less details as possible. Secondly, Gmail ask for an email address which needs to be filled with random and untraceable details. Post, acquiring an email, Gmail asks for a phone number and recovery email which are completely optional to provide. Lastly accepting all the terms and conditions, fake Gmail account has now created. (SMSBOWER, 2024)

**2) Facebook Account:** Post acquiring a fake email address from Gmail, Facebook requires some basic information which includes first name, surname, email address, password, DOB, gender, and phone number. After filling up the required information with fake or spoofed details, Facebook sends two validation codes on email and phone number to validate respective channels. The phone number which is used to create the fake account can be obtained using the attack vectors discussed above. (Kengly, 2023)

Furthermore, if an attacker created a spoof account of a victim's original account, they can actually give the same look and feel of the created profile by adding up victim's profile picture, background, pictures taken from original account, and adding up similar friends.

# IV. Design Specification

The solution uses a microservices architecture to implement 2FA authentication on both Signup and Login phase on the Facebook Platform. This architecture enhances the overall security and provides preventive measures on fake or spoofed identities as two forms of user identification are in place before giving access to the Facebook environment. Also, the microservices used are flexible to scalability and provides independent deployment of authentication components that ensures strong security without the compromise of user experience. Below-mentioned details helps to understand the proposed solution and its potential.

## IV. 1 Architecture

In Figure III, complete implemented architecture is explained with description and justification of each component's functionality:

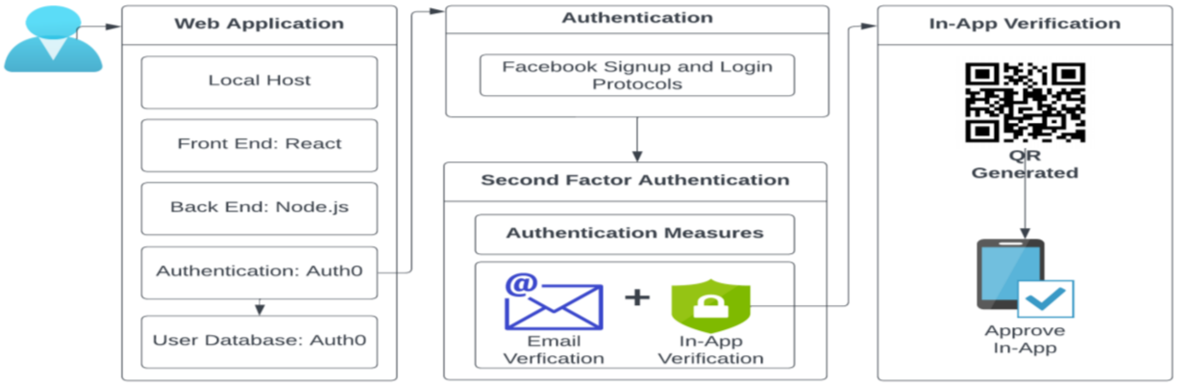


Figure III. Architecture Explained

**1) Host:** The solution is deployed using a shared platform where the user interface is hosted locally. Secondly, authentication details which is created with the Facebook authentication is stored under the Web-App "Auth0". Below table provides the specifications of both local and Web-App environment.

| Host Machine | |
|---|---|
| **Product** | LAPTOP-PMKF05PQ |
| **Processor** | Intel(R) Core(TM) i7-8550U CPU |
| **RAM** | 16.00 GB |
| **Operating System (OS)** | Windows 11 Home |
| **System Type** | x64-based processor |
| **Version** | 222H2 |
| **Web-Application** | |
| **Platform** | Auth0 By Okta |
| **Application** | Facebook-Dummy |
| **Client ID** | dev-1nrbcpqjspphhm0w.us.auth0.com |
| **Domain** | SUMElXBgGyv4HCU6loecDeHYAuzOcSqs |

Table I. Specifications Local and Web-App Environement

**2) FRONT-END:** React library is used for building the user interface as it allows to create an efficient and responsive web applications. Also, its component-based architecture can be compatible with diversified User Interface (UI) elements which provide complete access to developers to deploy effective solutions.

In this solution, React is providing an user interface to the overall setup where a login page is created which is supporting the complete functionality of the resolution.

**3) BACK-END:** Node.js provides a runtime environment which allows the developers to execute JavaScript codes on the server side which ensures high performance and scalable environment. This makes it ideal to develop fast and responsive back-end infrastructure as it can handle multiple connections simultaneously and efficiently. (Sample-01, n.d.)

All the coding of the user interface and the connection bridge is established with Web-App which is hosted on Auth0 for the login page is done using Node.js.

**4) AUTHENTICATION:** Auth0 is used as an authentication service and IAM (Identity and Access Management) which is used as the functionality to provide secure service for login / signup into Facebook account as second factor authentication. The 2FA offers validation from pre-created database based on the parameters derived from unique identity proofs provided by the respective countries to an individual such as national ID proof, passports, and driving license.

**5) IN-APP VERIFICATION:** This functionality works in both the signup and login phase where a QR (Quick Response) code is generated and gets scanned by the scanning mechanism during signup. This scanning validates user information from the associated Facebook account and cross-check it with the local database which contains information derived from respective national IDs. This complete setup provides an additional layer of security beyond using the passwords and validating email addresses. Further to login, setup uses a push notification mechanism to validate logins from untrusted devices.

# V. IMPLEMENTATION

This section provides a detailed step-by-step process that how implementation of the proposed solution is carried forward to ensure a secure and efficient 2FA system for both signup and login phase on the Facebook platform.

## V.I IMPLEMENTATION STEPS

**1) SETTING UP HOST ENVIRONEMENT:** The host machine is equipped with adequate resources which supports the smooth functionality of solution. Also, appropriate tools are installed such as React Library, Node.js with pre-installed PowerShell as the setup is running on Windows OS.

**2) DEVELOPING FRONT-END INTERFACE:** Using React library, new user interface is created which is efficient and responsive as it provides a Landing page for the web-server followed by the Login page which handles the complete authentication process of the deployed solution.

**3) BUILDING BACK-END INFRASTRUCTURE:** Various GitHub repositories are used in order to create and provide support to the front-end for the proper functionality of the setup. Node.js also provides an environment where it handles communication and operations on the server-side which in this case is Auth0 application.

**4) Aligning Authentication Service:** The Auth0 platform is used for its authentication and authorization capabilities which works under the login page of the created React project as it provides the complete support on the authentication of the users. This setup requires to create a web-application on Auth0 platform.

**5) Verifying Using Device Application:** This device or phone application verification provides two type of authentication, one for the Signup and second one for the login attempts made for Facebook Platform. To achieve this setup below steps to follow:

Once the above setup is established, secondary database needs to be created using the Auth0 database which will handle the functionality of verification on the desired terms for signup.

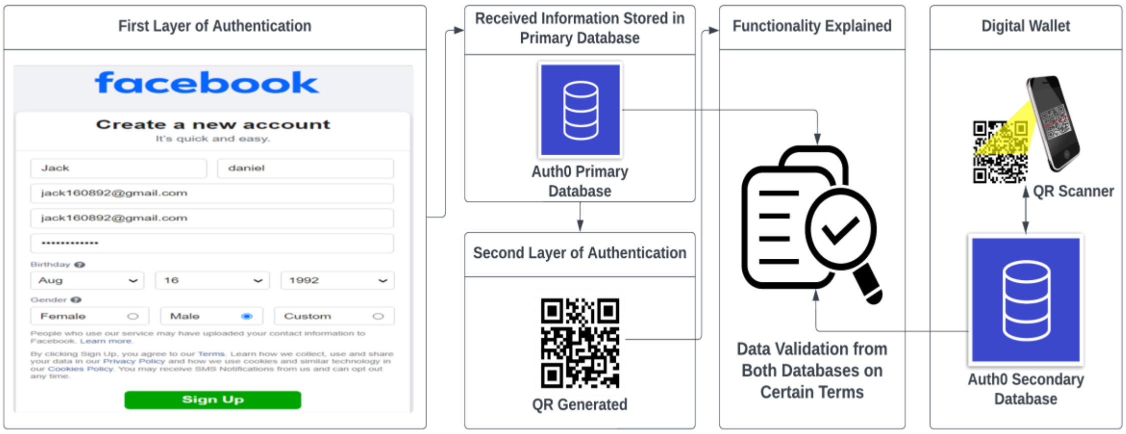
## V.II Authentication Flow

**1) User Registration:** The users provide their signup / login credentials for which they gets authenticated from Facebook. Based on the nature of the credentials, user will able to create an account or can login to a pre-existed account.

**2) User Creation:** Once the user confirms to be a legitimate part of Facebook's environment. Then, a user replica will be created on the Web-App with the information derived from Facebook Account such as full name, email address, DOB, phone number and Gender.

Another database needs to be created that aligns with the application that acts as a digital wallet (Guardian) which provides support to the verification procedure on specified terms. As mentioned above, these terms include data received from national ID proofs provided by respective countries with parameters such as ID number, name, email, DOB, Place of Birth, and phone number.

**3) Signup Authentication:** The authentication process works differently as it include security procedures implemented by Facebook followed by additional aligned protocols where user information gets validated from the pre-created secondary database for digital wallet for national IDs. The below provided figure elaborates the functionality of the authentication process for Signup:


First Layer of Authentication
facebook
Received Information Stored in Primary Database
Auth0 Primary Database
Second Layer of Authentication
QR Generated
Functionality Explained
Data Validation from Both Databases on Certain Terms
Digital Wallet
QR Scanner
Auth0 Secondary Database

Create a new account
It's quick and easy.

Jack | daniel
jack160892@gmail.com
jack160892@gmail.com
••••••••••••

Birthday
Aug | 16 | 1992

Gender
Female ○ | Male ● | Custom ○

People who use our service may have uploaded your contact information to Facebook. Learn more.

By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Privacy Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Sign Up

**Figure IV. User Validation and Authentication Explained**

**4) LOGIN AUTHENTICATION:** Post validating the user identity and successful creation of the account, solution provides another functionality of validation. This includes whenever user tries to login onto multiple different untrusted devices, every time user gets a push notification on their trusted smartphone which needs to be approved for login.

# VI. EVALUATION

This section provides evaluation of solution in terms of the research question proposed earlier "How strengthening of user validation on Meta platforms can mitigate fake accounts and enhance traceability of users for digital forensics". The research question focuses on enhancing user authentication on Meta Platforms which mitigates fake accounts and improves traceability while performing digital forensics. The below-mentioned information provides the significance of the  solution which as follows:

## VI.I EFFECTIVENESS IN MITIGATING FAKE ACCOUNTS

The solution opted significant approach which reduces the use and creation of fake accounts:

**1) ENHANCED USER VALIDATION:** The use of Auth0 environment provides authentication solution which in this case be aligned with two database. The primary database creates user and handles information be fetched from the created users on Facebook. Whereas, secondary database aligns with the application associated to represent as digital wallet (Guardian) which stores data derived from national IDs. By cross-checking the primary data with the data derived from trusted national databases, it reduces the likelihood of fraudsters or attackers creating fake accounts using fraudulent identities. This approach mitigates the use of fabricated or spoofed identities which directly decreases the count of fake accounts on the platform.

**2) MULTI FACTOR AUTHENTICATION (MFA):** The implementation of MFA practices on the login attempts using the similar application for user validation which provides enhanced security. This approach uses push notifications sent to user's registered device to authenticate login attempts made from unrecognized devices. This ensures that even if user's login credentials are compromised, still the unauthorized access be blocked which protects the account from being misused.

**3) ENHANCED TRACEABILITY FOR DIGITAL FORENSICS:** The solution directly enahnces the tracebility of user as their virual identity is directly bounds with their physical identity Proofs. This linkage provide the investigators and law enforcement officials with a proper channel to trace online activities back to real world identities. It also provides immense support when dealing with criminal investigations and violation of platform policies as this traceability ensures that responsible individuals can be identified accurately and held accountable for the events.

## VI.II CHALLENGES FACED

The solution provides significant advantages which straight away can be leveraged for the problem identified, but certain challenges must be acknowledged.

**1) GLOBAL APPLICABILITY:** The resolution depends on the availability and integration of national ID databases which is not same across all countries. But, most of the parameters on which the validation has been done by the solution is collected by most / all the countries to provide their citizens with national IDs.

**2) Privacy Concerns**: This challenge covers the user privacy concerns related to storage and management of sensitive information gathered under national ID information for Meta. This raise concerns on transparency on how data is collected, stored and used with regulatory frameworks such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), , Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) Framework, and more.

# VII. Conclusion And Future Work

The proposed solution effectively addresses the research question as it is enhancing the overall user authentication mechanism implemented on Meta Platforms. This is achieved by combining and bounding national ID verification method with MFA which creates a secure social-media environment, mitigates fake accounts and enhances the traceability of user actions for digital forensics.

Research work highlighted flaws and vulnerabilities associated with Meta's existing authentication processes as it is relying on third party applications such as email and telecommunication providers. On basis of that, new solution has proposed using the combination of legitimate database and 2FA for user validation. The solution showcase the potential that it can significantly reduce the count of fake accounts and improve the traceability of user activities which helps in cyber-criminal incidents and investigations.

Furthermore, research work identified insights on fake accounts that it not only hampers user experience but also affects the platform integrity with database stored with user information.

## VII.I Limitations And Implications

**1) Consideration Of Other Platforms:** The research primiarly focuses on implementing solution only on Facebook which left other platforms offered by Meta. However, solution is flexible and can be adapted by other platforms easily.

**2) Large-Dataset Implementation:** The prototype requires testing with numerous signup and login attempts from various networks to identify the true efficiency of the solution. This helps to find that the current solution is ready to be implemented in real-world or requires further corrections. But, solution only offered a prototype which helps to understand the mechanism of the proposed solution and if required to be implemented with Facebook's current posture, appropriate tools should be used in order to match the efficiency of the platform.

**3) Compliance With Regulatory Frameworks:** The secondary database, processes and stores complex user identity information which must be comply with various regulatory frameworks depending on the application is used in which region.

## VII.II Future Work

The study also needs to explore and design further solution for the challenges and limitations faced for the analysis of the current work if provided with more time:

**1) Digital Wallet Identity Integration:** By understanding and considering the complexity of storing crucial private information of national Ids under the regulatory frameworks for Meta Platforms. Another solution can be proposed which assigns a unique number offered by the application considered as digital wallet which further be provided to Meta to store it as a proof of identity shared for the particular verified user. This mitigates all challenges that Meta has to face and transfer all onto the application.

**2) Unified Meta Identity Solution:** This solution provides a unique identity number when user initially creates an account on any platform of Meta or based on this solution, on Facebook. This unique number provides a digital identity to user on Meta database which can be used to create accounts on Meta ecosystem such as Instagram and WhatsApp. Also by using this unique identifier, both platforms and user can take advantage of this unified experience which ensures that a single identity be used across all platforms. This solution enhances the need of single database rather than maintaining different databases for every other platform which ensures security, simplified account management, and interconnected user experience.

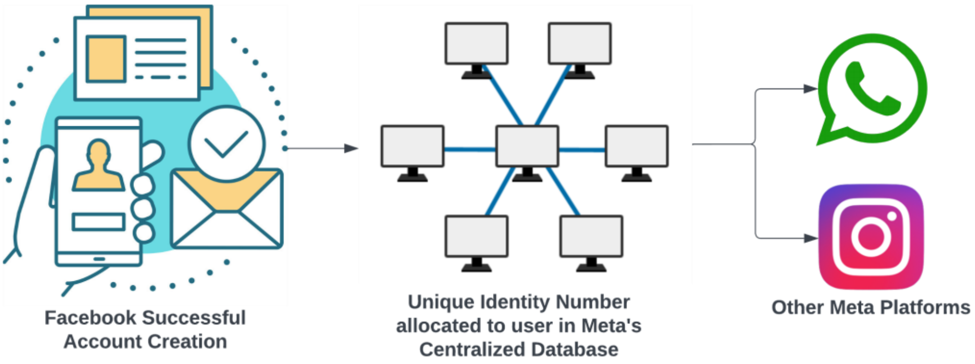

Facebook Successful Account Creation
Unique Identity Number allocated to user in Meta's Centralized Database
Other Meta Platforms

**Figure V. Unified Solution Explained**

# REFERENCES

Ahmad Rafi Ilzan, R. F. B. O. a. F. M. Y., 2023. *Understanding The Phenomenon and Risks of Identity Theft and Fraud on Social Media.* [Online]
Available at:
https://www.researchgate.net/publication/376607191_Understanding_The_Phenomenon_and_Risks_of_Identity_Theft_and_Fraud_on_Social_Media
[Accessed 07 July 2024].

Baruchin, R., 2024. *Why Fake Social Media Accounts are a Threat to Businesses Today.* [Online]
Available at: https://cyabra.com/blog/what-are-fake-accounts/#:~:text=These%20fake%20accounts%20serve%20to,the%20credibility%20of%20said%20entities.
[Accessed 09 July 2024].

Georgios Kontaxis, I. P. S. I. a. E. P. M., 2014. *Detecting social network profile cloning.* [Online]
Available at: https://www.researchgate.net/publication/224237161_Detecting_social_network_profile_cloning
[Accessed 08 July 2024].

Hallman, R., 2023. *SIM Swapping Attacks for Digital Identity Theft: A threat to financial services and beyond.* [Online]
Available at:
https://www.researchgate.net/publication/376612643_SIM_Swapping_Attacks_for_Digital_Identity_Theft_A_threat_to_financial_services_and_beyond
[Accessed 25 June 2024].

Ikhalia, E., 2013. *The need for two factor authentication in social media.* [Online]
Available at:
https://www.researchgate.net/publication/256667821_The_need_for_two_factor_authentication_in_social_media
[Accessed 04 July 2024].

Kengly, R., 2023. *3 Easy Ways to Make a Fake Facebook Account.* [Online]
Available at: https://www.wikihow.com/Create-a-Fake-Facebook-Profile
[Accessed 10 July 2024].

Mansooreh Karami, T. H. N. a. H. L., 2021. *Profiling Fake News Spreaders on Social Media through Psychological and Motivational Factors.* [Online]
Available at:
https://www.researchgate.net/publication/354139886_Profiling_Fake_News_Spreaders_on_Social_Media_through_Psychological_and_Motivational_Factors
[Accessed 08 July 2024].

Mary Madden, A. L. S. C. U. G. M. D. A. S. a. M. B., 2013. *Teens, Social Media, and Privacy.* [Online]
Available at: https://www.pewresearch.org/internet/2013/05/21/teens-social-media-and-privacy/
[Accessed 07 July 2024].

Mathew, A., 2020. *Threats and Protection on E-Sim.* [Online]
Available at: https://www.researchgate.net/publication/344065039_Threats_and_Protection_on_E-Sim
[Accessed 05 July 2024].

Mauro Conti, R. P. a. M. S., 2012. *FakeBook: Detecting Fake Profiles in On-Line Social Networks.* [Online]
Available at: https://www.researchgate.net/publication/261090651_FakeBook_Detecting_Fake_Profiles_in_On-Line_Social_Networks
[Accessed 08 July 2024].

Meta, 2019. *How Does Facebook Measure Fake Accounts?.* [Online]
Available at: https://about.fb.com/news/2019/05/fake-accounts/
[Accessed 10 July 2024].

Meta, 2024. *SEC Filings Details.* [Online]
Available at: https://investor.fb.com/financials/sec-filings-details/default.aspx?FilingId=17229405
[Accessed 05 April 2024].

Mohammad Mahyoob, J. A. a. M. A., 2021. *Linguistic-Based Detection of Fake News in Social Media.* [Online]
Available at: https://www.researchgate.net/publication/349850780_Linguistic-Based_Detection_of_Fake_News_in_Social_Media
[Accessed 09 July 2024].

Partha Chakraborty, M. M. S. M. N. M. K. A. a. P. C. T., 2022. *Fake Profile Detection Using Machine Learning Techniques.* [Online]
Available at: https://www.scirp.org/journal/paperinformation?paperid=120727
[Accessed 10 July 2024].

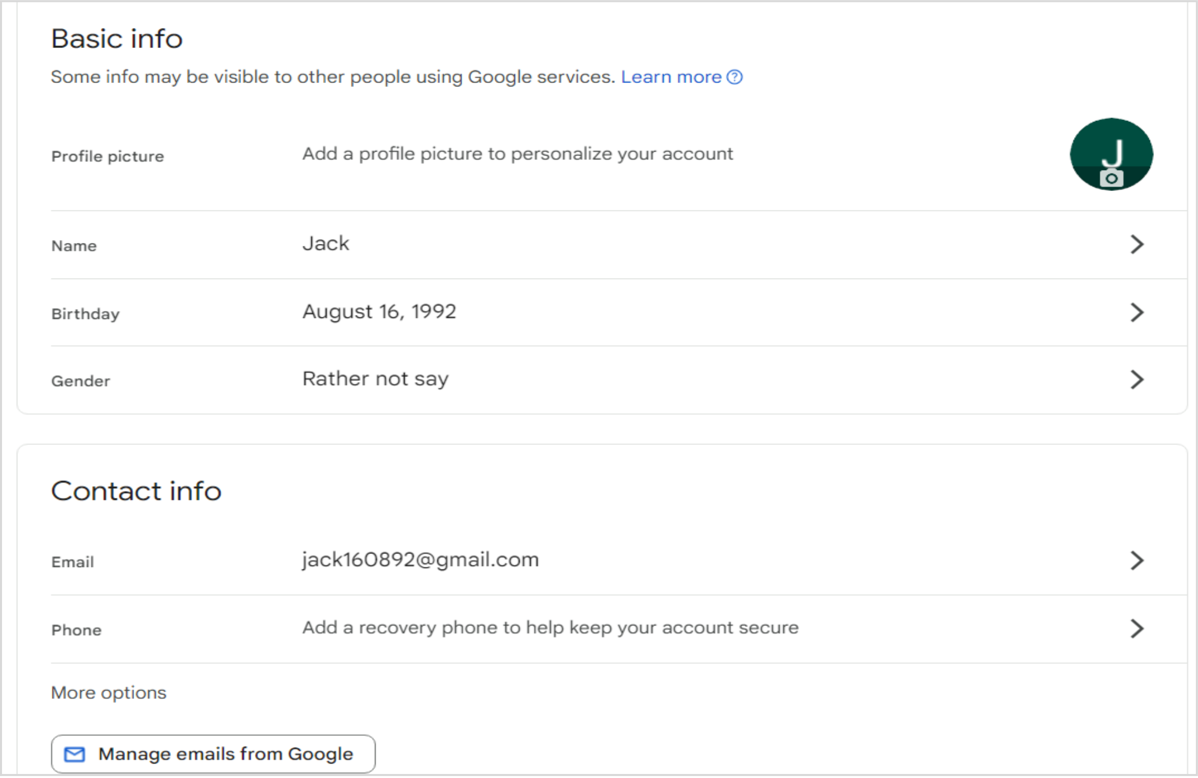
Sample-01, n.d. *auth0-samples / auth0-react-samples.* [Online]
Available at: https://github.com/auth0-samples/auth0-react-samples/tree/master/Sample-01
[Accessed 15 July 2024].

Schröder, J., 2019. *Influencer Fraud on Instagram - A Descriptive Analysis of the World's Largest Engagement Community (Master Thesis by Jonas Schröder).* [Online]
Available at: https://www.researchgate.net/publication/337651456_Influencer_Fraud_on_Instagram_-_A_Descriptive_Analysis_of_the_World's_Largest_Engagement_Community_Master_Thesis_by_Jonas_Schroder
[Accessed 31 June 2024].

SMSBOWER, 2024. *How to Make a Fake Gmail Account: Step-by-Step Guide.* [Online]
Available at: https://medium.com/@smsbower/how-to-make-a-fake-gmail-account-step-by-step-guide-6ca86b425cd1#:~:text=To%20create%20a%20fake%20Gmail%20account%2C%20users%20need%20to%20follow,email%20to%20ensure%20successful%20creation.
[Accessed 10 July 2024].

Zacky Althero, J. S. a. A. O., 2023. *Blockchain Technology for Authentication and Validation Social Network Accounts.* [Online]
Available at: https://journal.pandawan.id/b-front/article/view/358
[Accessed 09 July 2024].

# APPENDIX



## Basic info

Some info may be visible to other people using Google services. Learn more

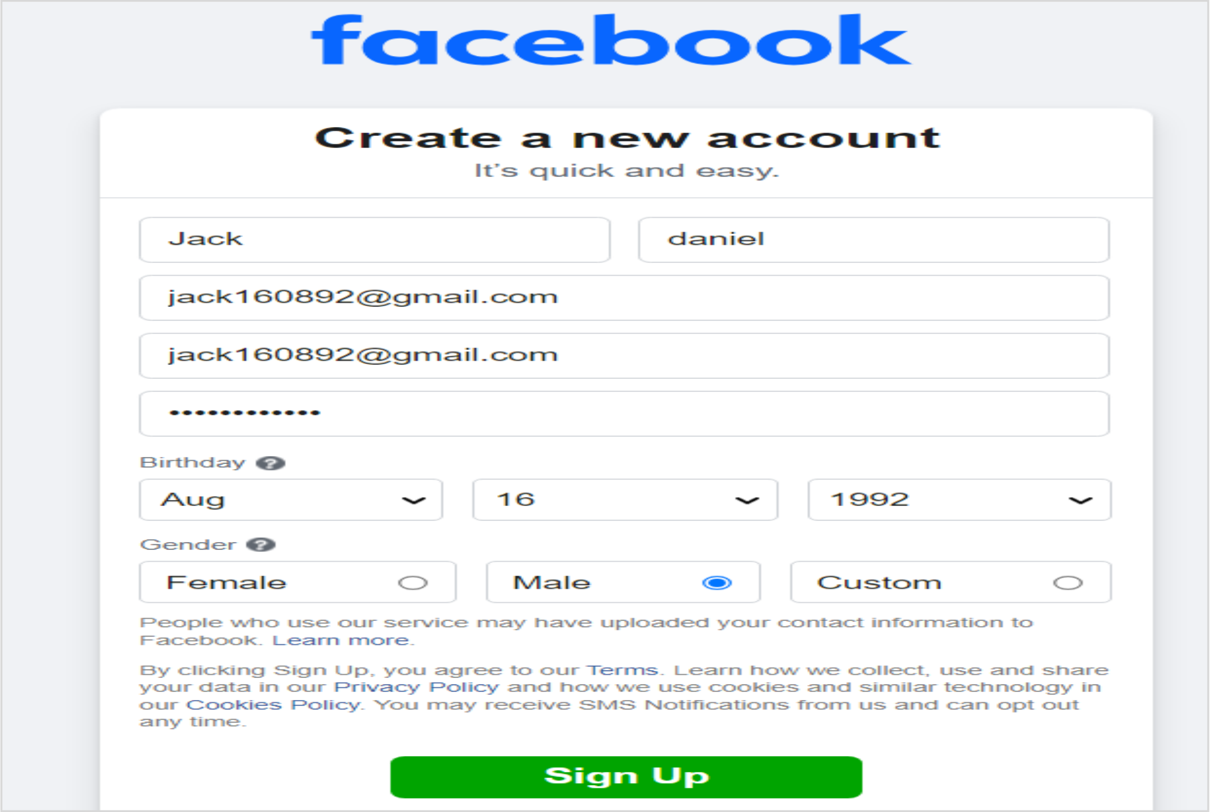
| | |
|---|---|
| Profile picture | Add a profile picture to personalize your account |
| Name | Jack |
| Birthday | August 16, 1992 |
| Gender | Rather not say |

## Contact info

| | |
|---|---|
| Email | jack160892@gmail.com |
| Phone | Add a recovery phone to help keep your account secure |

More options

Figure VI. Creation of Fake Gmail Account with Untraceable Information



## Create a new account

It's quick and easy.

Jack | daniel

jack160892@gmail.com

jack160892@gmail.com

•••••••••••••

Birthday

Aug | 16 | 1992

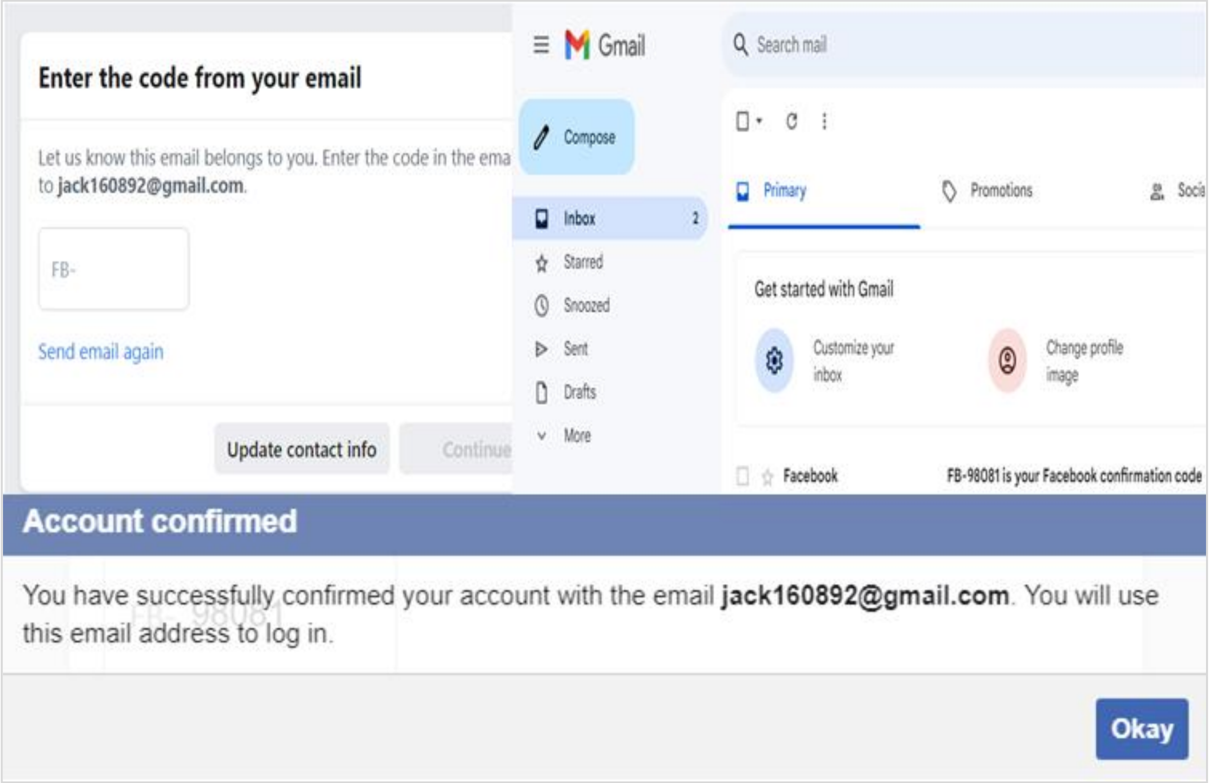
Gender

Female ○ Male ● Custom ○

People who use our service may have uploaded your contact information to Facebook. Learn more.

By clicking Sign Up, you agree to our Terms. Learn how we collect, use and share your data in our Privacy Policy and how we use cookies and similar technology in our Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Figure VII. Creation of Fake Facebook Account with Fake Gmail Address



Enter the code from your email

Let us know this email belongs to you. Enter the code in the ema to **jack160892@gmail.com**.

FB-

Send email again

Update contact info  Continue

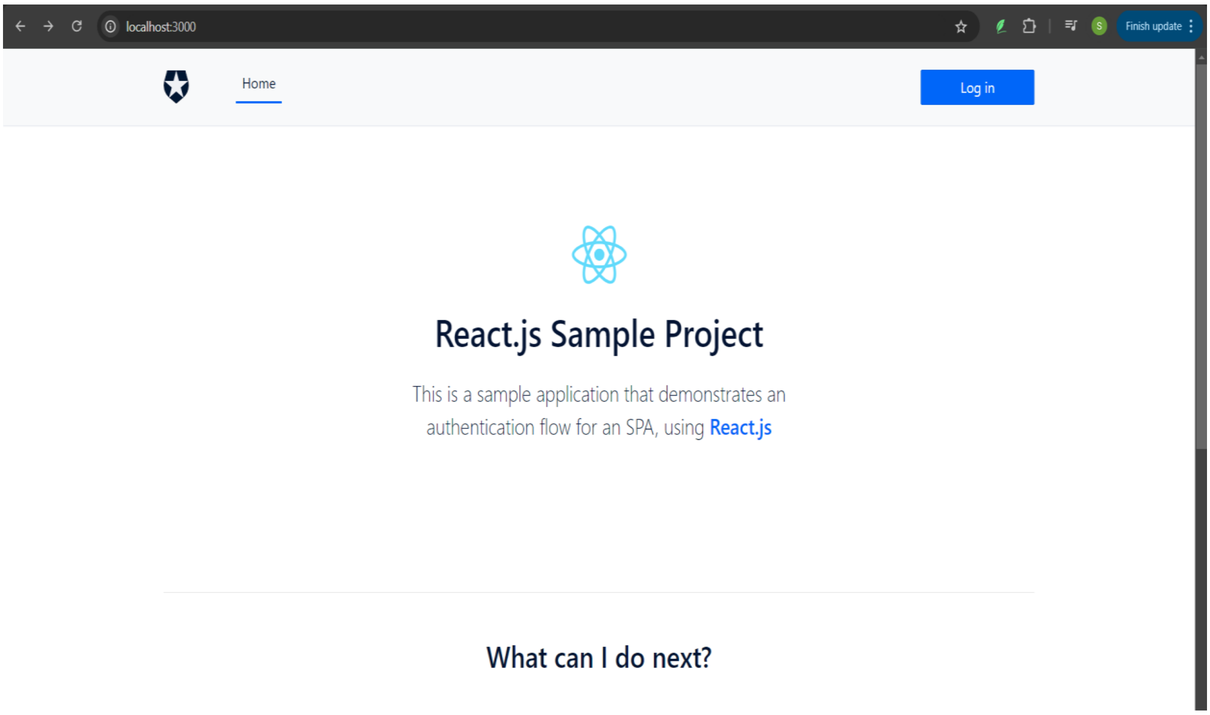
Facebook FB-98081 is your Facebook confirmation code

**Account confirmed**

You have successfully confirmed your account with the email **jack160892@gmail.com**. You will use this email address to log in.

Okay

**Figure VIII. Facebook Account Validation of Provided email**



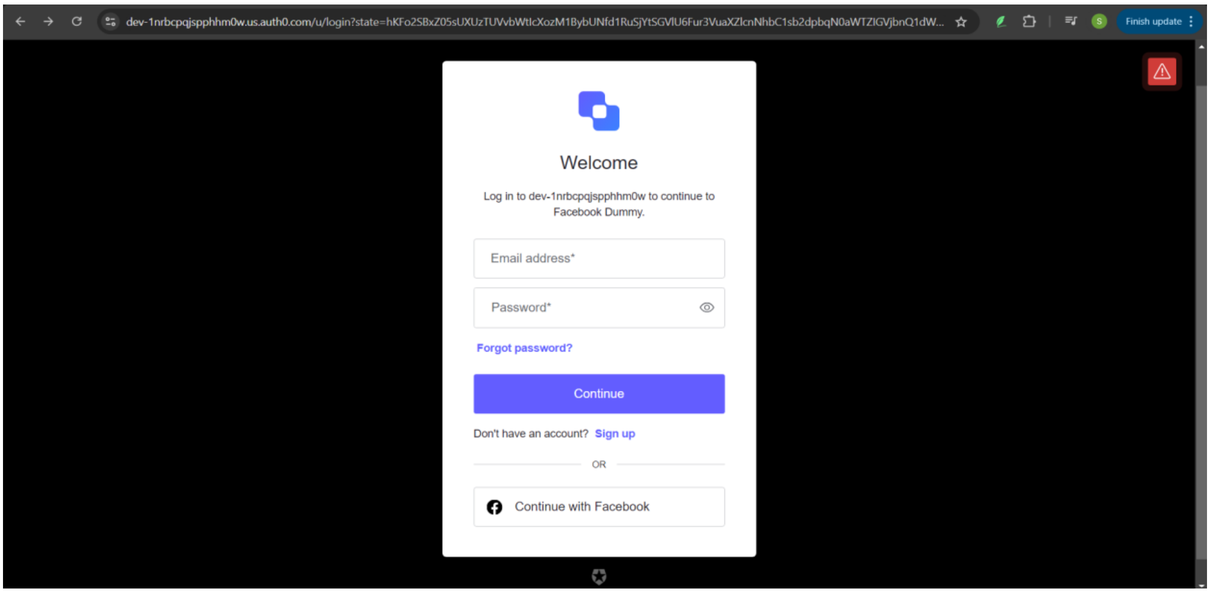
localhost:3000

React.js Sample Project

This is a sample application that demonstrates an authentication flow for an SPA, using React.js

What can I do next?

**Figure IX. User Interface Home / Landing Page**



dev-1nrbcpqjspphhm0w.us.auth0.com/u/login?state=hKFo2SBxZ05sUXUzTUVvbWtlcXozM1BybUNfd1RuSjYtSGVlU6Fur3VuaXZlcnNhbC1sb2dpbqN0aWTZIGVjbnQ1dW...

Welcome

Log in to dev-1nrbcpqjspphhm0w to continue to Facebook Dummy.

Email address*

Password*

Forgot password?

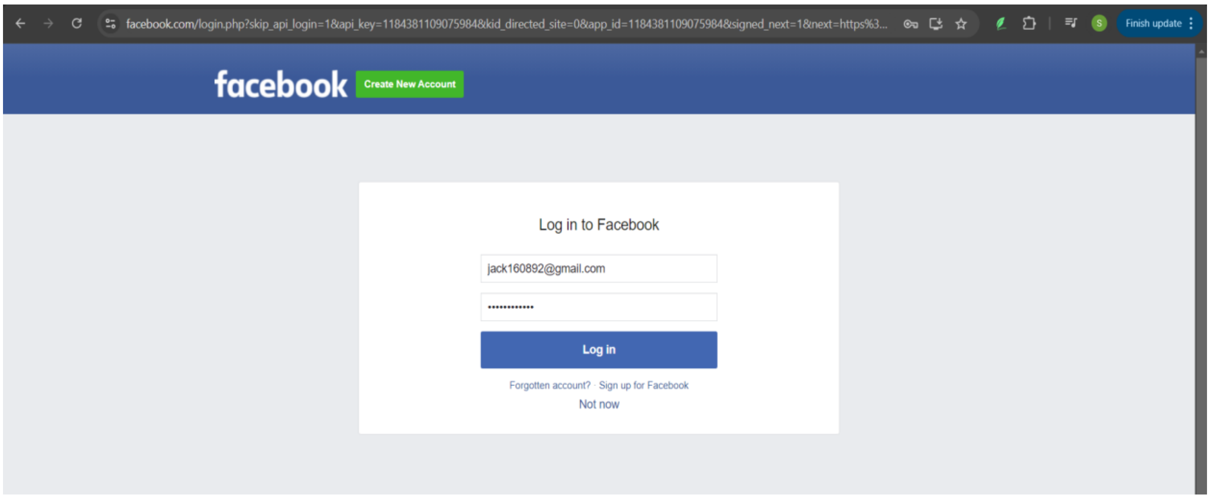
Continue

Don't have an account? Sign up

OR

Continue with Facebook

Figure X. Login / Authentication Page



facebook.com/login.php?skip_api_login=1&api_key=1184381109075984&kid_directed_site=0&app_id=1184381109075984&signed_next=1&next=https%3...

Log in to Facebook

jack160892@gmail.com

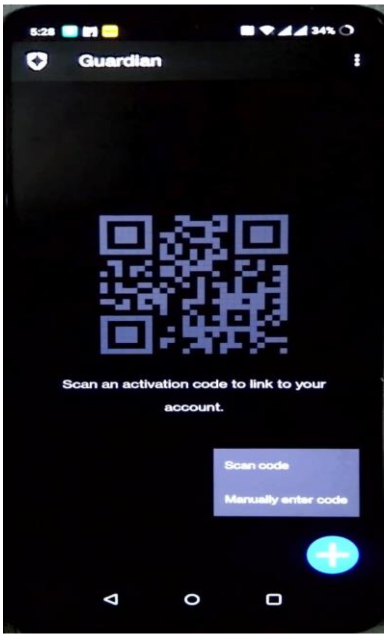
••••••••••••

Log in

Forgotten account? Sign up for Facebook

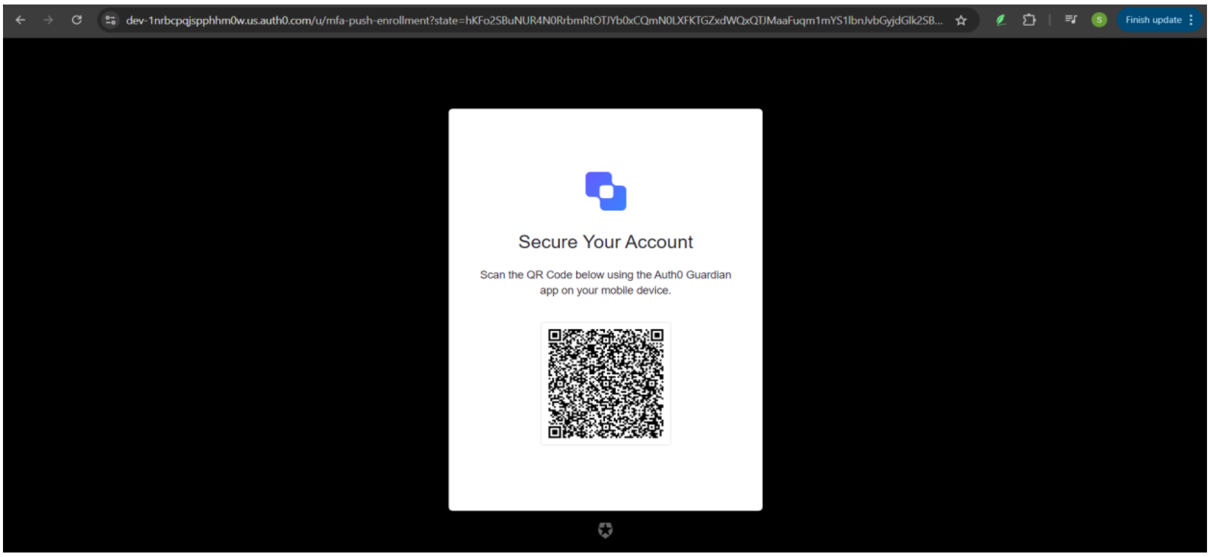
Not now

Figure XI. Facebook Official Login Page



Scan an activation code to link to your account.

Figure XII. Digital wallet Scanning Mechanism

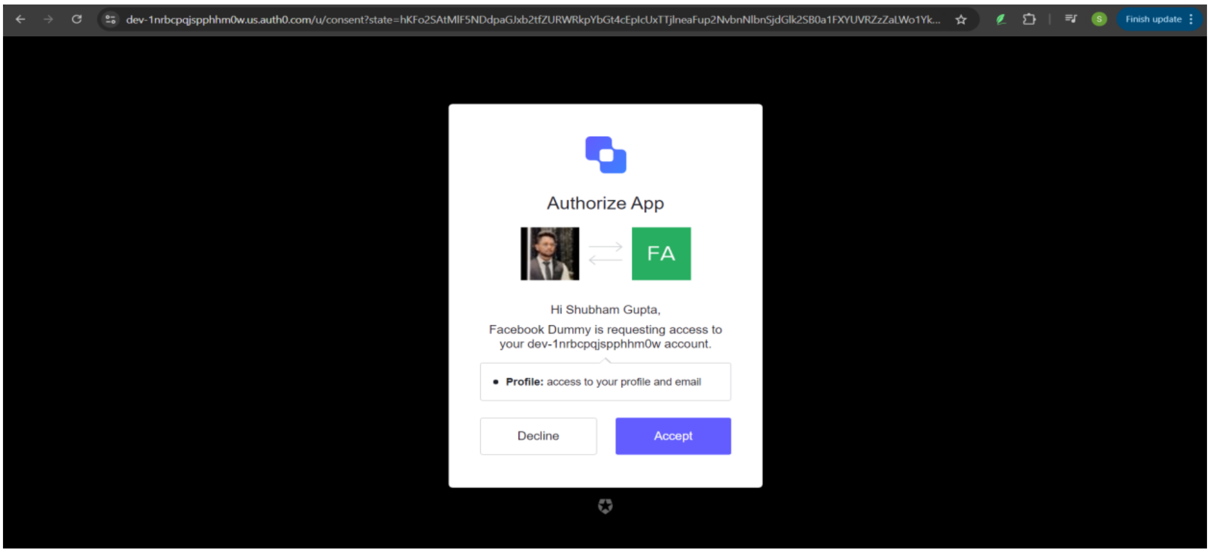


dev-1nrbcpqjspphhm0w.us.auth0.com/u/mfa-push-enrollment?state=hKFo2SBuNUR4N0RrbmRtOTJYb0xCQmN0LXFKTGZxdWQxQTJMaaFuqm1mYS1lbnJvbGyjdGlk2SB...

Secure Your Account

Scan the QR Code below using the Auth0 Guardian app on your mobile device.

Figure XIII. Scanner Provided by Primary Database For Authentication



dev-1nrbcpqjspphhm0w.us.auth0.com/u/consent?state=hKFo2SAtMlF5NDdpaGJxb2tfZURWRkpYbGt4cEplcUxTTjlneaFup2NvbnNlbnSjdGlk2SB0a1FXYUVRZzZaLWo1Yk...

Authorize App

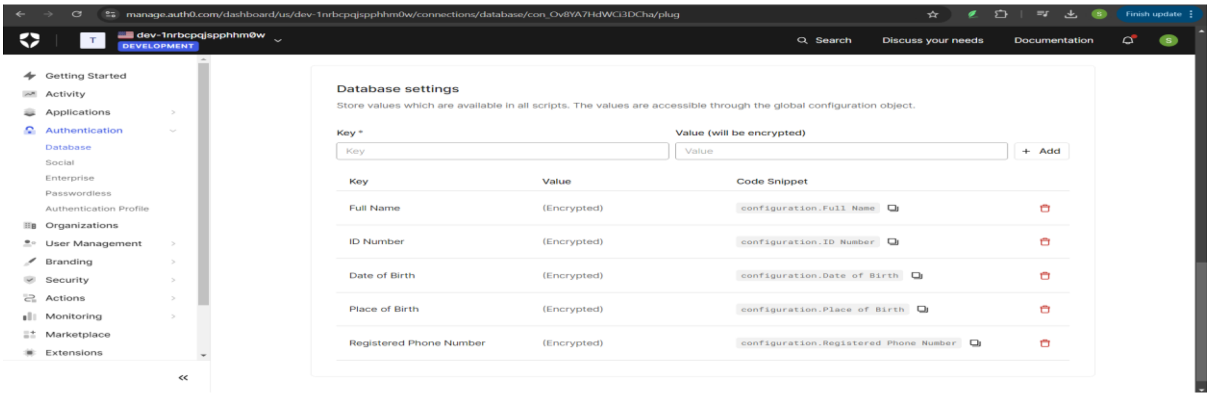
Hi Shubham Gupta,

Facebook Dummy is requesting access to your dev-1nrbcpqjspphhm0w account.

- **Profile:** access to your profile and email

Decline | Accept

Figure XIV.  Primary Database Information Fetch



manage.auth0.com/dashboard/us/dev-1nrbcpqjspphhm0w/connections/database/con_Ov8YA7HdWCi3DCha/plug

Database settings

Store values which are available in all scripts. The values are accessible through the global configuration object.

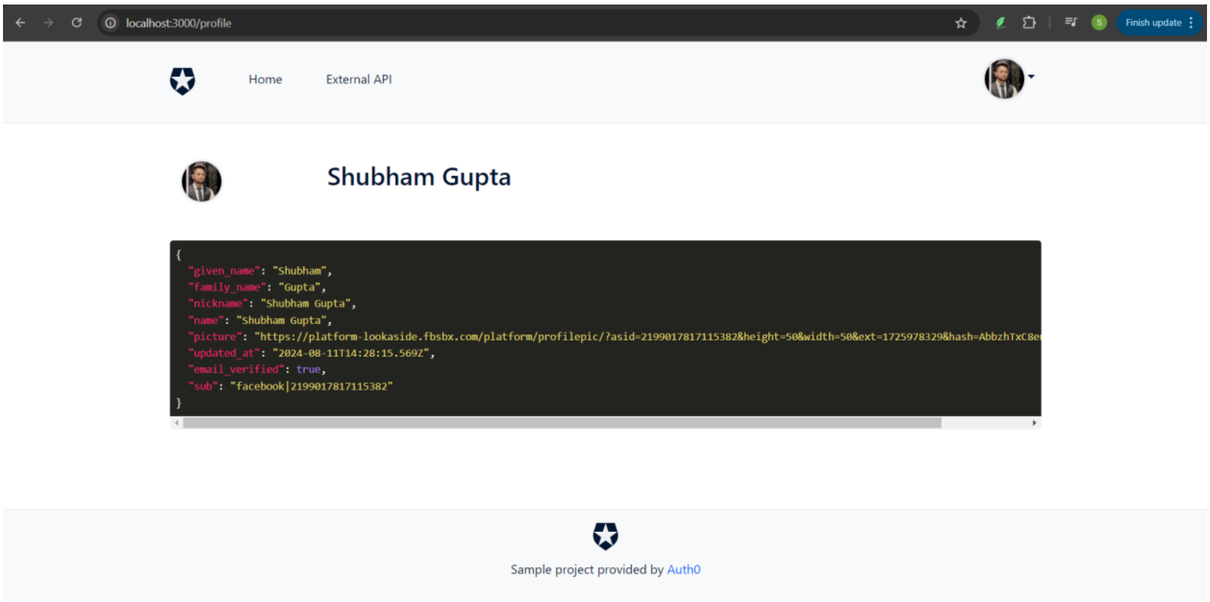
Key * : Key

Value (will be encrypted) : Value

+ Add

| Key | Value | Code Snippet |
|---|---|---|
| Full Name | (Encrypted) | `configuration.Full Name` |
| ID Number | (Encrypted) | `configuration.ID Number` |
| Date of Birth | (Encrypted) | `configuration.Date of Birth` |
| Place of Birth | (Encrypted) | `configuration.Place of Birth` |
| Registered Phone Number | (Encrypted) | `configuration.Registered Phone Number` |

Figure XV. Secondary Database Attributes



```
{
  "given_name": "Shubham",
  "family_name": "Gupta",
  "nickname": "Shubham Gupta",
  "name": "Shubham Gupta",
  "picture": "https://platform-lookaside.fbsbx.com/platform/profilepic/?asid=2199017817115382&height=50&width=50&ext=1725978329&hash=AbbzhTxC8e
  "updated_at": "2024-08-11T14:28:15.569Z",
  "email_verified": true,
  "sub": "facebook|2199017817115382"
}
```

Figure XVI. Web-App Side Verification

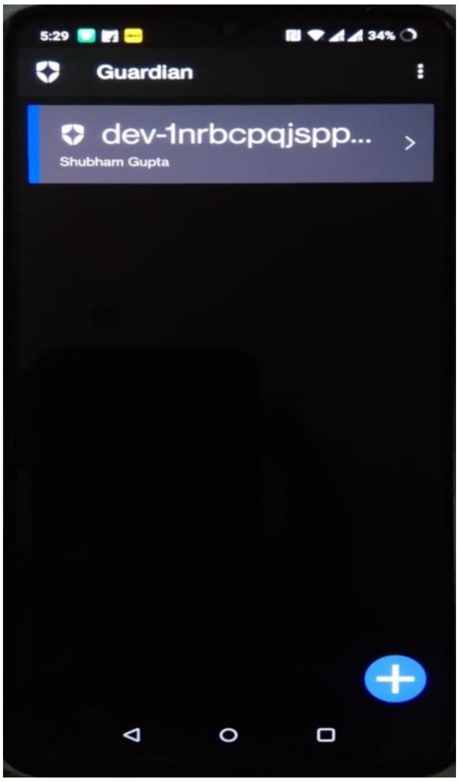


Figure XVII. Trusted Device Side Verification