JOURNAL OF BASIC AND APPLIED SCIENCES

Content and Specifications Development of a Next Generation Network Communication System for Location Identification

Bunakiye Japheth*, and Juliana Consul[2]

ARTICLE INFORMATION

Original article

Received: February 23, 2026
Revised form: June 18, 2026
Accepted: June 23, 2026
Published: June 25,2026

Available online:

Citation: Bunakiye Japheth and Juliana Consul (2026) **Content and Specifications Development of a Next Generation Network Communication System for Location Identification**

[1] Department of Mathematics and Computer Science, University of Africa Toru-Orua; bunakiye.japheth@uat.edu.ng
[2] Department of Mathematics, Niger Delta University; ji.consul@ndu.edu.ng
* Correspondence: bunakiye.japheth@uat.edu.ng; Tel.:+2348061324564

Abstract

The development in this paper aims to set a new standard in telecommunication, providing users with reliable, secure, and high-quality services while enabling operators to efficiently manage and optimize their networks. It is intended to revolutionize the way telecommunication networks handle the identification and management of user locations. This system integrates related technologies to provide enhanced services, including accurate location tracking, improved call quality, and robust security features. The project focuses on building a scalable and efficient infrastructure that leverages the latest advancements in network communication such as Google location feature, RESTful APIs, GPS Integration and Voice over IP (VoIP) provision. The system is designed with a modular architecture to allow for easy integration and scalability of the features. The RESTful APIs provides APIs for communication between services and external applications, the GPS integration utilizes GPS technology for real-time location tracking, and Voice over IP (VoIP) supports VoIP for high-quality voice communication.

Keywords: Next Generation Network (NGN); Identification of user locations; Management of user locations; On Boarding Screen; JSON Web Token

1. Introduction

1.1 The Next Generation Network (NGN) denotes a packet-switched network capable of delivering telecommunication services alongside data and mobility support. It can utilize various broadband capabilities, particularly Quality of Service (QoS)-enabled transport technologies, wherein service-related functions operate independently of the underlying transport technologies. Currently, distinct networks serve various purposes, including voice, data, and different forms of video. Telephony, Internet, and cellular networks represent distinct domains, each possessing its own protocols and services. The concept of the Next Generation Network (NGN) entails a singular network that transmits all varieties of data and delivers services in packet form akin to those utilized on the Internet ((Gürfidan *et al.,* 2023). This project aims to reduce the time required to determine and prioritize various service levels in next-generation networks (NGN) by offering a complementary service for users.

Key theoretical foundations this paper is leveraging on include concepts from telecommunications, network architecture, quality of service (QoS), and security. With this foundations, specific alignments are created to further explain the functionality of an application that is capable of locating network users within the defined framework. The user experience specification utilizes the associated theories within the incorporated internet protocol service addressing scheme. This is followed by an evaluation template that takes care of the application accessibility fundamentals. The technical standards handle the issues of metadata, data quality, interoperability and data format (Yücel & Açikgöz, 2023). These are issues of concern for the data provisioning and integration. The entire design concept is such that the callers will not be able to see each other's locations but the server side design will enable the service sequence to read the locations of the callers with the associated identities.

2. Materials and Methods

2.1 The User Experience and Connecting Formalities

This section explains the content and specifications development. It entails the user experience of the system and the specifications involving the user interface (UI), the front end (FE), and the backend (BE) connecting formalities.

2.1.1 User Experience Specifications

The UI, which uses Figma basically guides the entire app creation process. From the front-end to the back-end with outlined specifications and detailed guides and steps involved to bring the entire app to life. At this stage we have the User Interface (UI), Front-end and Back-end. While, the Front-end and Backend uses React Native and Nodejs to interconnect and interrelate for the application to meet with the intended objectives, the User Interface carries the entire project from conceptualization to implementation testing (Homssi *et al.,* 2023). The basic interface here is the On Boarding Screen as shown in figure 1.

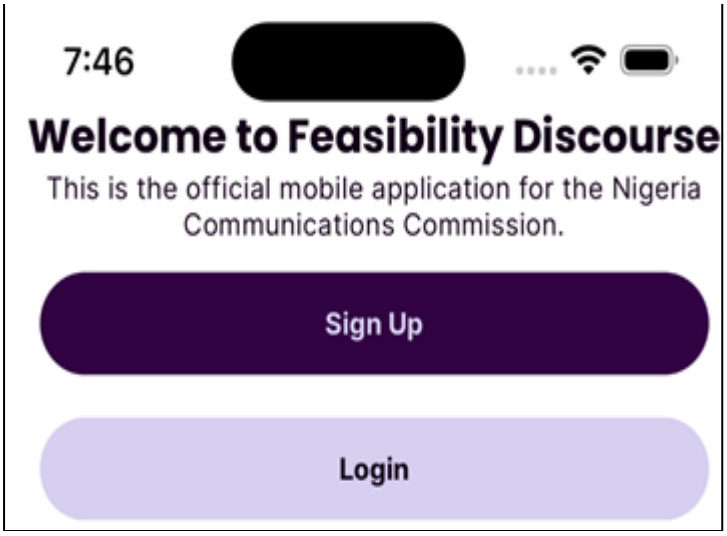

Figure 1. On- Boarding Interface

Through this stage, the user is been prompted to create a personal profile using the Sign Up option. The User profile screen displays details about the user, such as the user's name, email address, mobile number, etc. which can also be updated. The front-end basically enables users to get authenticated (login) and also create accounts as new users (signup) using their email addresses and other Single Sign-On (SSO) options (Rachakonda *et al.,* 2024). The user is then prompted to update his/her account by providing name and phone number (to be verified), enabling him/her to explore other screens such as Contacts, Contact Details, Audio/Video Call, etc. as shown in figures 2.

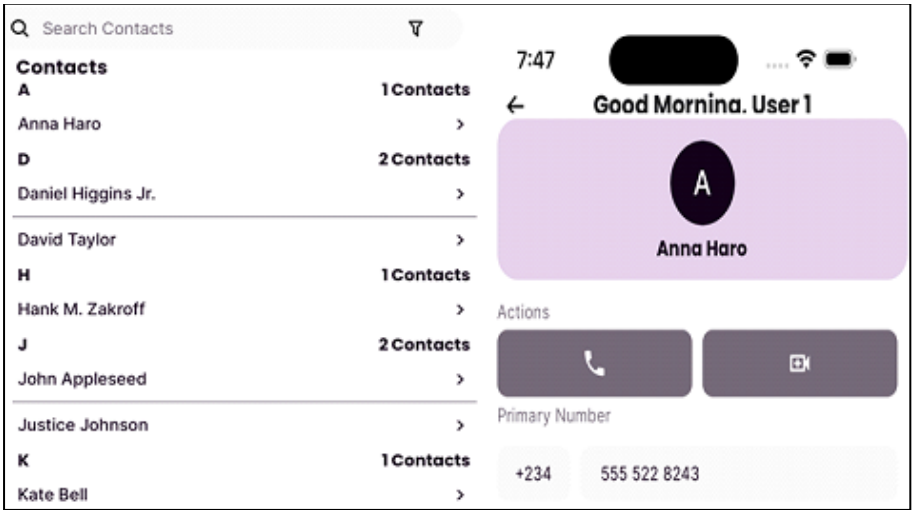

Figure 2. Contact and Contact Details

Afterwards the user can navigates further to settings in order to have access to configure other features to suit any particular purpose as the situation demands (Ali *et al.,* 2023). A user can also communicate (audio and video calls) with other users who has registered and authenticated accounts, using that user's mobile number stored on their device. Also, on every incoming call, a notification pops up to alert the target user as shown in figure 3.

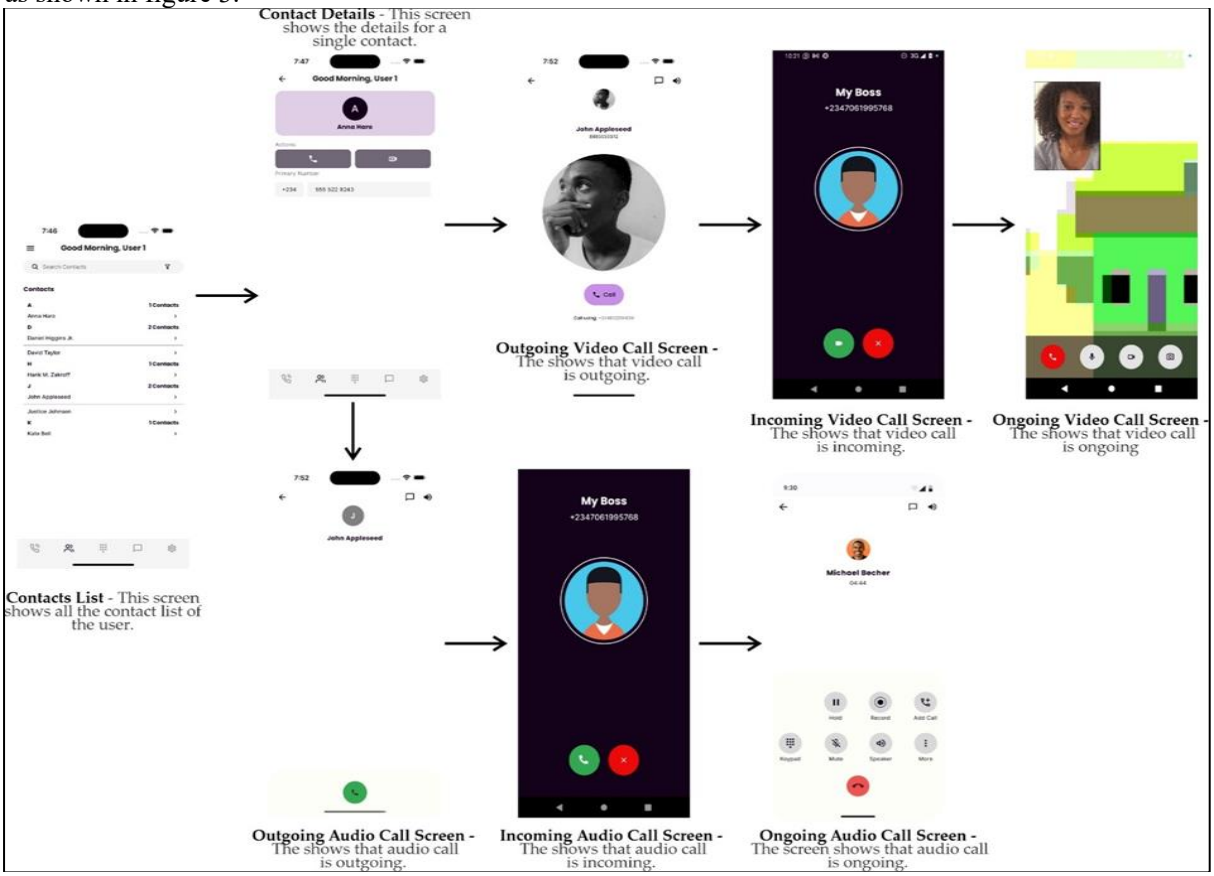

Figure 3. Pop up Call Notifications

The backend is a monolithic server that at first enable the registered admin user to navigate the Dashboard as shown in figure 4.

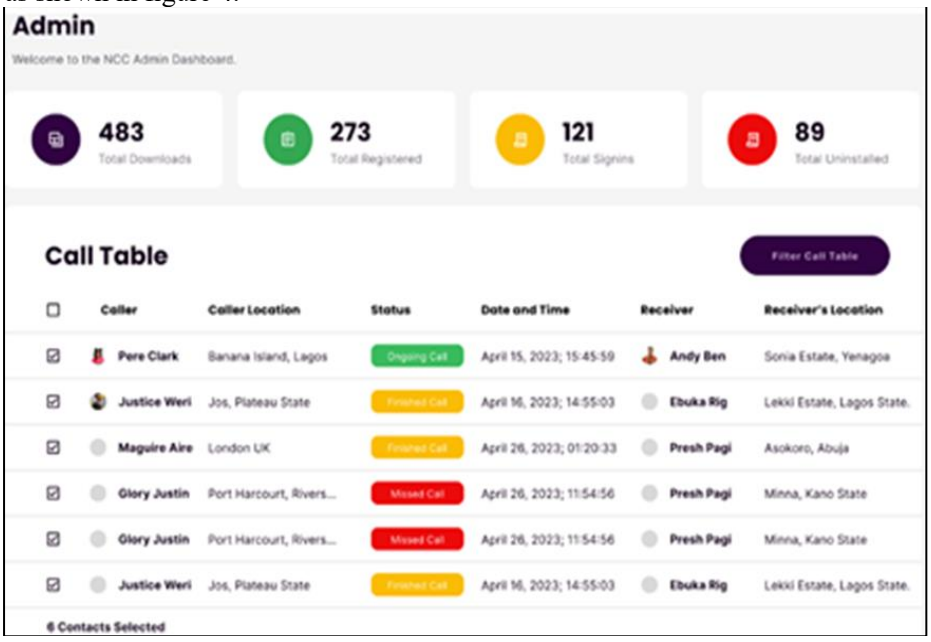

Figure 4. Admin Dashboard

For administrative purposes (server), a laptop computer can be used. The application is suitable for different target platforms (IOS and Android). Both Android and IOS devices can be used for signal testing in terms of communication (audio and video call) (Savunen *et al.,* 2023). The monolithic server performs three basic operations:

1. Operation 1 - User Authentication & Authorization
2. Operation 2 - User Communication (Audio and Video)
3. Operation 3 - User Notification

2.2 User Authentication & Authorization

The User Authentication & Authorization service routes carries the logic of registering and logging users by:

a. Asking for an email address
b. Sends an One-time-password (OTP) code to the inputted email address
c. Then, if the email address exists, the OTP code is copied and inputted in the app for verification
d. Once successful, the user with the email address is registered and prompted to update his/her account by adding a name and phone number, and also verify if the phone number is valid
e. Afterwards, the user provides a password to further allow him/her login
f. Then, the user is allowed to login with his verified email address and password
g. Once successful, a JWT (JSON Web Token) is generated to authorize the user to access other routes meant for users

2.3 User Communication (Audio and Video)

The User Communication service allows authorized users to make audio and video calls to other users with the same app. This part Auto detects users' location and other relevant information of both users for every connection either initiated or joined and displays it on the server (Gürfidan *et al.,* 2023). The User Communication Routes carries the logic of creating a communication instance either video or audio, if a call is initiated, with the following properties:

* user – The one who initiated the call
* userCallLoc – The location of the user
* mate – The one who joined the call
* mateCallLoc – The location of the mate
* status – The status of the user or mate either missed, incoming or outgoing
* callType – The type of the call either audio or video
* callStatus – The status of the call either missed, ongoing or finished

The logical sequence in this service auto detects the location of the user and mate, by using a middleware passed to the routes which creates the communication instance, which gets the longitude and latitude of where the call is been initiated and connected (Petroulakis *et al.,* 2023). That is, auto detects users' location and other relevant information of both users for every connection either initiated or joined and displays it on the server. It also allows authorized users to make audio and video calls to other users with the same app.

2.4 User Notification Service

The User Notification Service routes incorporate a firebase service with a client identity (id) and private key_id to provide a messaging service to send/receive notifications and messages (Gürfidan *et al.,* 2023). With this firebase service created, two basic logics are created for a notification to be sent or received.

i. registerForPushNotifications: This logic registers a user for receiving or sending a notification
ii. call Notification: Allows the registered user to send or receive a notification

Majorly alerts prompts users for an incoming call and other relevant messages such as app updates, etc. Whenever the app is installed in a mobile device (Android or iPhone), a registered user can make calls either videos or audio, making it possible for the server to auto-detect their locations. Remember that provided, the app has been installed on a device and the user did not make use of the app for calls; the server will also detect their locations. After successful download of the app from the Google Play Store, and the moment a user has registered and successfully created an account on the application, the app will create a *background service* which is not displayable [UI] that will auto detect the location of the users even when the app is not used to initiate or join a call (Ahmad *et al.,* 2023).

3. Results and Discussion

3.1. Content on Connecting Formalities

Commonly NGNs are built around Internet Protocol (IP). That's why sometimes NGN is referred to as an all-IP network to describe the transformations towards the future. This application in this current development is centered on dedicated service IPs addressing, evaluation template and configurations, data Integration for congestion control and security measures incorporation as shown in figure 5.

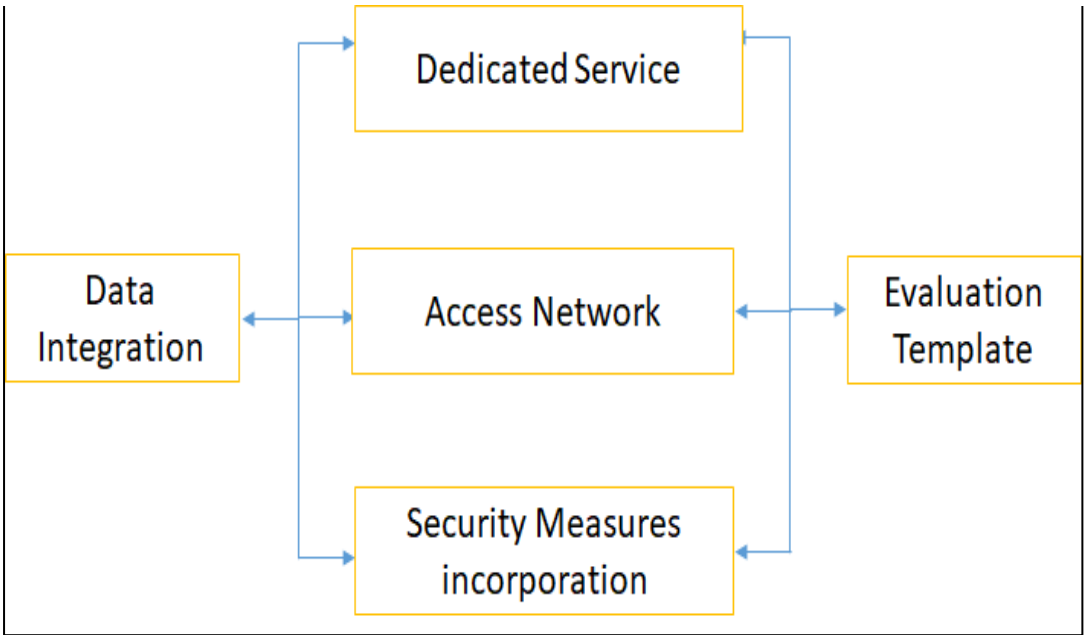

Figure 5. Components Interrelationship

3.2 Dedicated Services

Currently the application can be downloaded from the Google Play store, which means the IP addressing configurations are dedicated to making it accepted by Google Play store. The dedicated services are such that the bundle has to be uploaded to Google Play store (Yücel & Açikgöz, 2023). Also, a privacy policy which contains how the user's information is been managed and used in the app has to be provided and, if the application requires authentication (register & login process), a valid test credential is also provided for the Google Play store developers team to access and test the functionality and validity of the app. Countries/regions that are allowed to gain access to the app, the targeted audience were chosen, and the kind of sector our app is meant for, such as entertainment, logistics or communication etc. The sustainability of our app depends on how accessible it is to Google Play store developers for continuous testing and checking for both our privacy policy and the validity of the test credentials provided earlier in order to deal with malicious content (Savunen *et al.,* 2023). The evaluation template is showcased here to ascertain the utility of the app from the point of getting it from the Google Play store and subsequent applicable priorities by the users. The entire process is described in the subsections respectively. Profile data integration for congestion control explains what makes communication to be possible with our app even in circumstances where there is much traffic in the network. Our app uses Web Real Time Communication (WebRTC) technology. With WebRTC, real-time communication capabilities were added to the application that works on top of an open standard. It supports video, voice, and generic data to be sent between peers, allowing developers to build powerful voice- and video-communication solutions. Security measures incorporation is concerned with the core values of the app (Rachakonda *et al.,* 2024). The location detection is carried out with users allowing their GPS setting to be used by our app. Although, the location detection as a security measure is currently a work in progress, our team of developers are working tirelessly to ensure this can be managed in order to enforce location detection with or without user's consent. However, for user and device security, after email verification, and a user has entered his/her name following the provision of a valid mobile number, the user now has to set a password for his/her account as shown in figure 6.

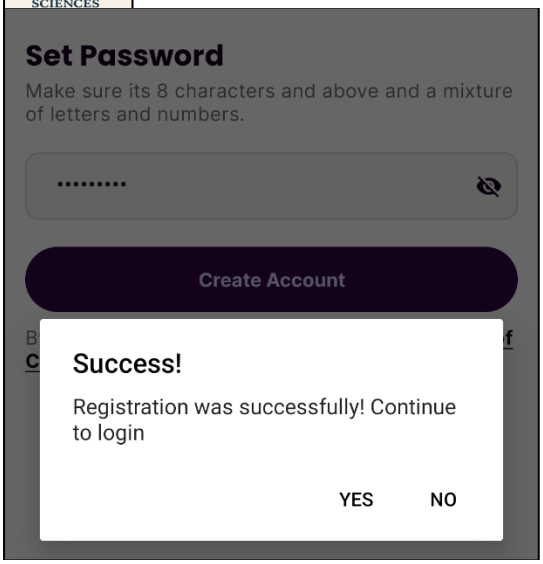

Figure 6. Password Protection Setting

At the point of dedicating the IP addressing scheme in the system, the policy component will evaluate the pricing/billing, data model, data lexicon, data access, custodianship and privacy issues with regards to users' position (Ridhawi *et al.,* 2020). These functionalities could be exploited through the use of mobile phones access to the network and the use of the information. Accessing the network is of great concern as services may now allow authorized person to have real-time information on the location of a mobile user duly certified with our app as shown in figure 7.

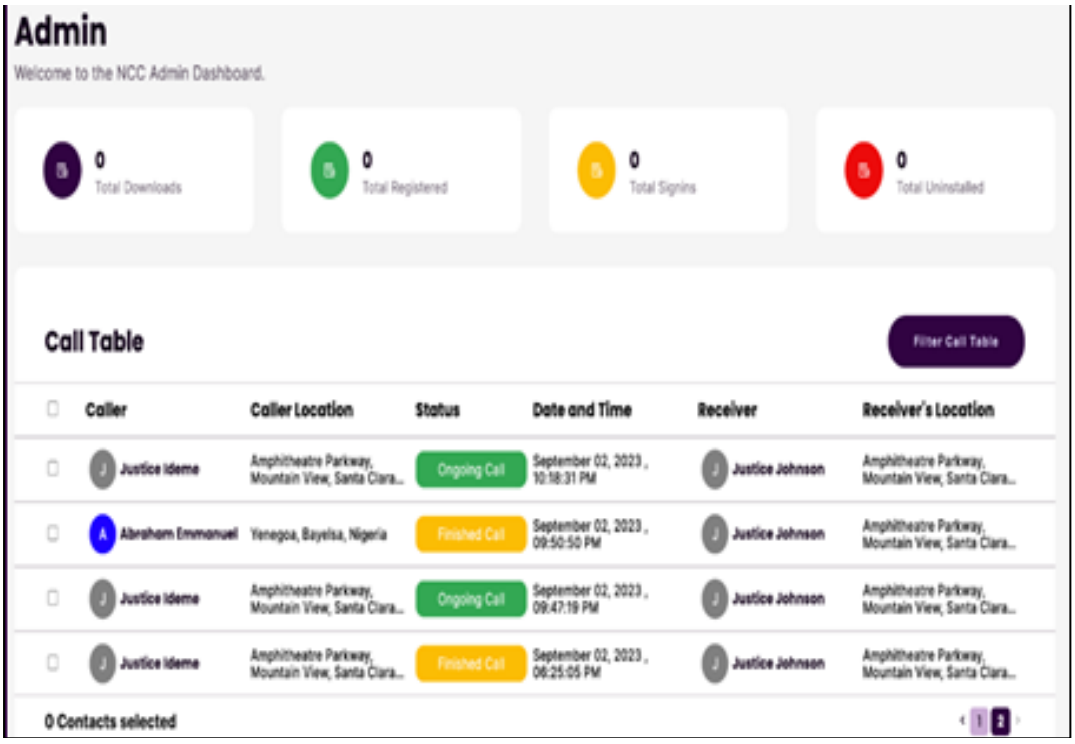

Figure 7. Authorized Service to Identify User Location

The technical standards handle the issues of metadata, data quality, interoperability and data format. These are issues of concern for the data provisioning and integration. For the access network component, issues of network scalability, the billing method, response time, data volume, data formats and content are handled (Saravanan *et al.,* 2025). The data component includes the issues of data quality (accuracy of the data information), data model and formats. Using the built in app location permission (GPS), which shares users (caller and receiver) location information (Homss *et al.,* 2023), the server side with the location permission

been allowed, a longitude and latitude is decoded and stored in our database as the users location as illustrated in figure 8.

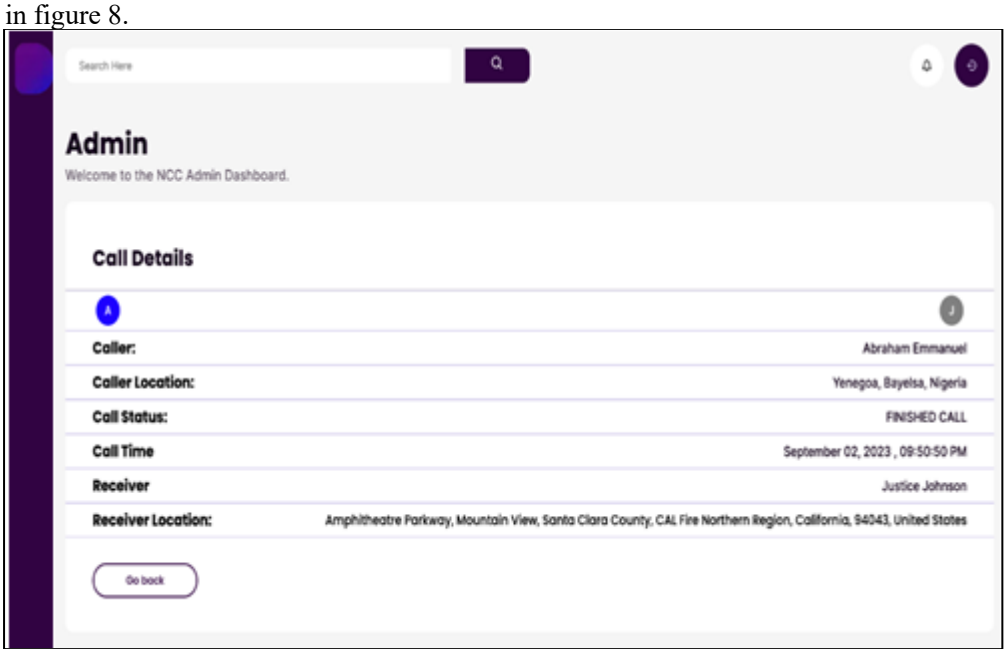

Figure 8 Specific Call Information

4. Conclusion

This app when finally deployed will be a location-based service designed to curb insecurity in Nigeria and beyond. As stated earlier the App can now be downloaded from the Google play store and carefully follow the evaluation steps to ensure that it is serving the purpose for which it is created. These steps achieved so far can cater for actual development of first sample software solution for quality assurance management and then moving forward the quality assurance metrics can be tested by using the App to communicate.

5. Patents

Author Contributions: *All authors contributed to the development of the manuscript*

Funding: *The research is funded by the Institution Based Research (IBR) scheme of the Tertiary Education Trust Fund (TETFUND)*

Data Availability Statement: *This published article contains all of the data that was examined throughout this investigation.*

Acknowledgments: *The authors extend their appreciation to TETFUND for funding this research through the Institution Based Research (IBR) domesticated in the Niger Delta University with a Grant Number: TETF/DR&D/UNI/POLY/YENAGOA/RG/2020/VOL.1*

Conflicts of Interest: *The authors declare no conflicts of interest.*

Nomenclature: *Not applicable.*

References

Ahmad, R., Hämäläinen, M., Wazirali, R., & Abu-Ain, T. (2023). Digital-care in next generation networks: Requirements and future directions. *Computer Networks*, *224*, 109599.

Al Homssi, B., Dakic, K., Wang, K., Alpcan, T., Allen, B., Boyce, R., & Saad, W. (2023). Artificial intelligence techniques for next-generation massive satellite networks. IEEE Communications Magazine, 61(9), 58-64. https://doi.org/10.1109/MCOM.001.2200777

Al Ridhawi, I., Otoum, S., Aloqaily, M., Jararweh, Y., & Baker, T. (2020). Providing secure and reliable communication for next generation networks in smart cities. Sustainable Cities and Society, 56, 102080. https://doi.org/10.1016/j.scs.2020.102080

Ali, S. A., Elsaid, S. A., Ateya, A. A., ElAffendi, M., & El-Latif, A. A. A. (2023). Enabling Technologies For Next-Generation Smart Cities: A Comprehensive Review and Research Directions. *Future Internet*, *15*(12), 398.

Gürfidan, R., Ersoy, M., & Kartal, H. (2023). Use of Artificial Intelligence in Next-Generation Wireless Network Infrastructures. *Türk Mühendislik Araştırma ve Eğitimi Dergisi*, *2*(2), 104-112.

Petroulakis, N., Mattsson, M. O., Chatziadam, P., Simko, M., Gavrielides, A., Yiorkas, A. M., & Bogdanova, A. (2023). NextGEM: next-generation integrated sensing and analytical system for monitoring and assessing radiofrequency electromagnetic field exposure and health. *International Journal of Environmental Research and Public Health*, *20*(12), 6085.

Rachakonda, L. P., Siddula, M., & Sathya, V. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*, 100220.

Saravanan, M., Ajayan, J., Parthasarathy, E., & Ramkumar, V. (2025). Architecture and Future Trends on Next Generation Networks. *Resource Management in Advanced Wireless Networks*, 19-43.

Savunen, T., Hämmäinen, H., Kilkki, K., & Kekolahti, P. (2023). The role of mobile network operators in next-generation public safety services. *Telecommunications Policy*, *47*(3), 102489.

Yücel, M., & Açikgöz, M. (2023). Optical communication infrastructure in new generation mobile networks. *Fiber and Integrated Optics*, *42*(2), 53-92.