Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

ITMAHuB2023

https://kppim.uitm.edu.my/research/conferences/itmahub-2023

2nd International Conference on Information Science, Technology, Management, Humanities, and Business

Hotel UiTM, Shah Alam, Malaysia, 26-27 Sep. 2023

Organised by College of Computing, Informatics and Mathematics, UiTM, Malaysia

SAPP: The Game-Changer in Nigeria's Battle against Insecurity and Emergency Delays

John Dah, Norhayati Hussin*, Muhamad Khairulnizam Zaini, Divine Senanu Ametefe

** Corresponding Author*

College of Computing, Informatics and Mathematics,
Universiti Teknologi MARA (UiTM), 40150 Puncak Perdana, Selangor, Malaysia

J. Dah 2020864844@isiswa.uitm.edu.my; N. Hussin yatihussin@uitm.edu.my; K. Zaini nizam0374@uitm.edu.my; D. Ametefe 2019813378@isiswa.uitm.edu.my
Tel: +601172527269

Abstract

In Nigeria, pervasive insecurity, characterized by Boko Haram massacres, suicide bombings, Fulani herder genocides, abductions, and armed robberies, has led to massive loss of life and property. Traditional approaches like curfews, states of emergency, and military checkpoints have proven inadequate, primarily due to late emergency call responses caused by the inability to quickly identify dangerous zones. Utilizing a Design Science Research methodology, this study designs, develops, and evaluates the Security and Prompt Protection (SAPP) mobile application. SAPP is engineered to bridge these security gaps by enabling victims in perilous situations to instantly alert both loved ones and security agencies, while simultaneously providing their real-time geographical location for immediate, targeted assistance

Keywords: Safety and Security, Nigeria Insurgency, Emergency concerns, Security Application, Real-time tracking

DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5458

1.0 Introduction

Nigeria has been grappling with the significant security threat posed by Boko Haram, which opposes western education (Afzal, 2020; Adesoji, 2010). They've caused significant casualties and made international headlines with their abduction of 276 schoolgirls in 2014 (Giovanni, 2014). Other security challenges in Nigeria include the Fulani herders' conflicts, kidnapping, bombings, and theft, with an alarming increase in kidnappings over the past decade (Nya, 2018; The Global Kidnapping Epidemic Index, 2022) and a high ranking in global terrorism (Afzal, 2020; Global Terrorism Index, 2018). This unrest has stymied economic and social progress (Adebakin, M. A. Raimi, 2012; Sheriff F. Folarin, 2014). Though countermeasures have been initiated, the security challenges persist. The rapid technological evolution, especially in mobile phones, offers a potential solution (Vijayakumar et al., 2017; Qureshi et al., 2021; Acheampong, 2021; Dah & Hussin, 2021). Other nations have adopted security apps, like "Go Safe" in India for women's safety (Varsha & Srikanth, 2017), or hardware-integrated solutions like the "Women Security Mobile App" (Miriyala et al., 2016). Given Nigeria's widespread smartphone usage and the absence of a prominent digital security solution, this ongoing study aims to develop a Safety Application (SAPP) to address Nigeria's security woes. The envisioned SAPP will also provide live monitoring for any situation, not just security threats. Howbeit, this article will specifically report on the design and development of as part of the Design Science research

eISSN: 2398-4287 © 2024. The Authors. Published for AMER and cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers and cE-Bs (Centre for Environment-Behaviour Studies), College of Built Environment, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/e-bpj.v9iSI18.5458

method adopted in the overall study. The evaluation of the SAPP, which includes an empirical evaluation of its acceptance is yet to be carried out, hence it will be captured in this work. Thus, this study aims to achieve the following objectives.
1) To design and develop a Safety Application (SAPP) tailored to Nigeria's unique security landscape.
2) To leverage mobile technology for enhanced security and emergency response.
3) To provide a comprehensive solution for real-time monitoring and alert in various emergency scenarios.

Driven by the promise of mobile applications in addressing safety and security issues and recognizing the challenges Nigeria faces with security and the limited success of current countermeasures, this study aims to leverage smartphones for a digital solution. Considering the widespread smartphone usage in Nigeria and the absence of a notable security platform, this study proposes the development of a Safety Application (SAPP). This application won't just address security threats but will also offer live monitoring features for users in various contexts. The key contributions of this work include:

1) To the best of our knowledge, this is one of the first applications developed to counter the insecurity situations embargoed by the Nigerian populace.
2) The proposed SAPP application renders real-time safety notifications and live location of troubled victims.
3) The design of the proposed SAPP application ensures simplicity of usage and integrates eighteen possible security and emergency concerns.
4) The general set-up of the proposed SAPP application will serve as a form of timely notification to friends, families and law enforcement agencies about unpleasant situations encountered by citizens or foreigners.

The rest of this paper is stratified into four parts. Section 2 showcases the proposed methodology. Section 3 proffers and discusses the experimental results obtained. Finally, the study is concluded in section 4.

2.0 Methodology

2.1 Materials and Components
The various facets harnessed for developing the proposed SAPP comprise of the software-based and hardware-based elements, encompassing various components such as the Android Studio IDE, google Firebase, emulators, mobile phones and GPS.

A) Integrated development environment (ide)
The Android Studio IDE is owned by Google Inc. (Singh, 2014). It's the official platform for building Android apps, automobile devices, Android OS laptops, and wearable gear like smartwatches and bands. Gradle-based build system, emulator, and code templates power Android Studio. For this study, the IDE supported Java (Ribeiro et al., 2021). Figure 1 shows android studio's IDE.

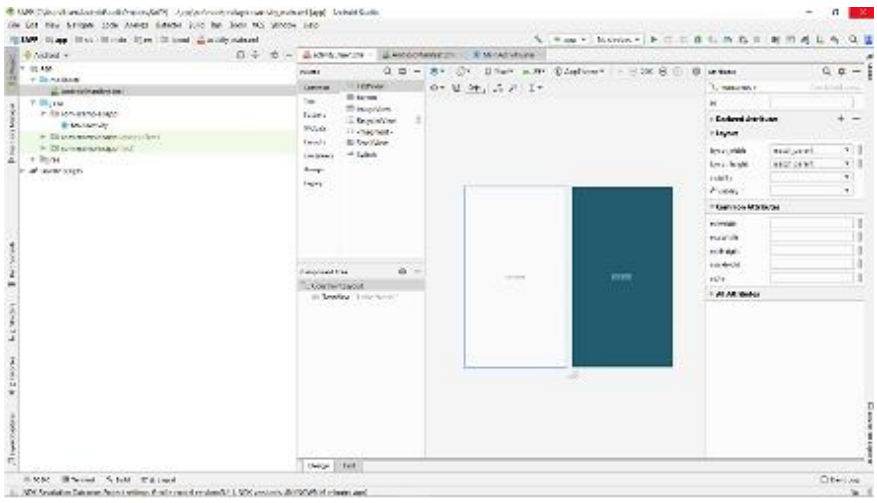

Figure 1. Android Studio Integerated Development Environment (IDE)

B) Emulators
Emulators mimic computer systems because they allow computer applications to run on their interfaces. Also, they help to play out and exhibit written code at any step in the development process (Singh, 2014; Yang et al., 2019). This study employed two emulators. First, Genymotion (S. Wu et al., 2018), which is an open-source Emulator for Windows and Mac OS mobile developers. The study also uses an SM-G973F Sam-sung Galaxy S10 hardware emulator. Figure 2 shows software-based and hardware-based emulators.

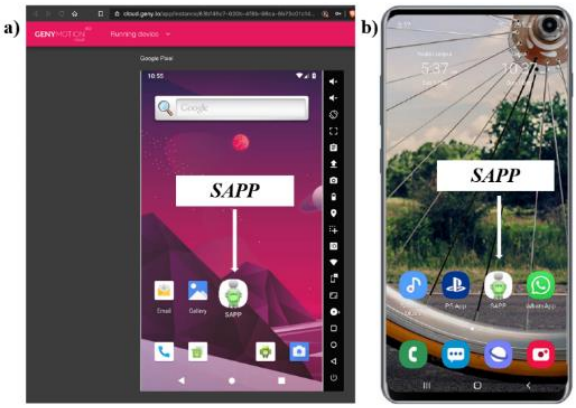

Figure 2. (a) Genymotion software-based emulator (b) SM-G973F Samsung Galaxy S10 hardware-based emulator

C) Firebase real-time database

Databases are designed not only for storage but also for the organization, protection, and distribution of data (Moroney, 2017). This study employs Google's Firebase, a cloud-hosted, real-time database that facilitates instantaneous data sharing in JSON format (Khawas & Shah, 2018). The real-time feature of Firebase, combined with its open-source nature and its provision of free services for several projects, makes it an optimal choice for this research.

D) Rationale for materials, tools, and methodology selection

The chosen development tools and databases were open-source and easily accessible, ensuring cost-effectiveness. Android Studio was selected as the IDE for its robust features and compatibility with Firebase and Android (Singh, 2014; Ribeiro et al., 2021). Emulators like Genymotion and Samsung Galaxy S10 provided an effective testing platform (S. Wu et al., 2018; Yang et al., 2019). Firebase's real-time capabilities and its seamless integration with Android made it an optimal choice (Khawas & Shah, 2018). The study utilized the Design Science Research (DSR) methodology to create and assess the SAPP, aiming to address security concerns effectively (Hevner et al., 2004).

2.2 SAPP Workflow Process

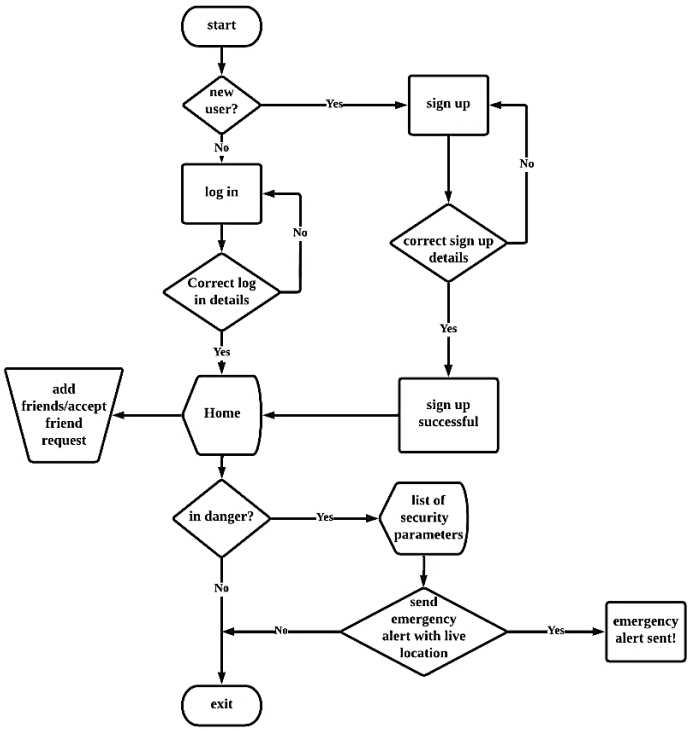

Figure 3. Proposed SAPP functionality

Figure 3 illustrates the sequential operation of the proposed SAPP system. Upon launching, users encounter a login interface. If login details are valid, users access the home page; otherwise, they are returned to the login page. Unregistered users are directed to

a registration page. The system checks registration details for accuracy, either confirming the registration or prompting corrections. Once successfully logged in or registered, users reach the SAPP homepage, where they can access various functionalities.

- Add friends (emergency contacts that would be notified in times of danger)
- Receive friend requests, send an emergency alert (notify emergency contacts of potential danger or request for help)
- Receive emergency alerts (receive emergency notifications from contacts of potential danger or requests for help)
- Track friends' live locations (monitor the live location of your emergency contacts to know their locations in real-time)
- View security parameters

2.3 Use Case of SAPP

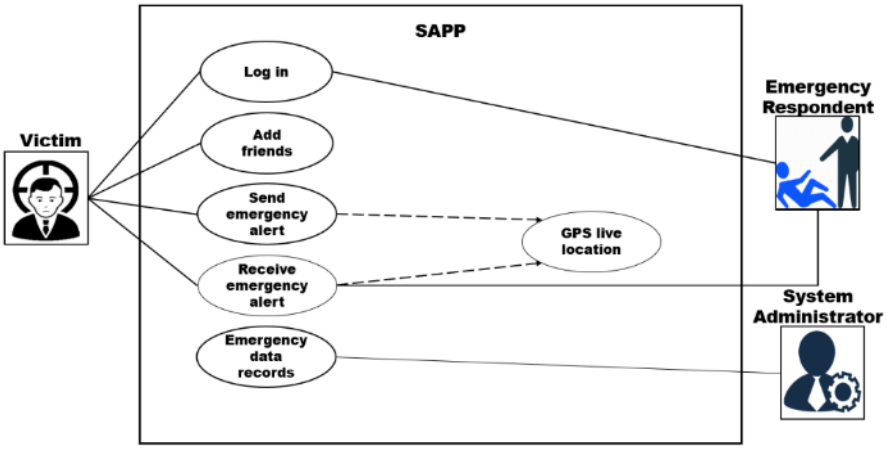

Figure 4. Proposed SAPP use case

Figure 4 illustrates the used case of the proposed SAPP application. It contains three actors that can initiate, interfere with, or control the functions and operation of the SAPP. These parties are classified into two, they are;

- Personal user(s)
- Administrative user(s)

Personal users of the App, intended for safety and security, can be categorized as either the "first user" (victim) or the "second user" (emergency respondent). The victim initiates distress alerts during threats, while the emergency respondent receives them. Roles can reverse based on the situation. Distress alerts also share the victim's live location, with options for sending texts and media. Multiple emergency contacts can be notified simultaneously. On the other hand, the administrative user manages the system's back-end activities. They don't engage in alerts but oversee all SAPP operations. They can be individuals or groups with tasks that encompass;

- Manage registered users (view the number of registered users and their data)
- Manage emergency data (view and monitor most frequent reported security concerns)
- Monitor unauthorized activities (warn, delete and block users who abuse the services)
- Manage user access credentials (reset user's password and retrieve login de-tails)
- Maintain services (periodic maintenance to ensure app functions as appropriate)

2.4 Layouts and UI Interfaces

A) Home UI and layout

Figure 5. (a) Emulated Home activity interface (b) Back-end code layout and design of home interface

The UI interface is simply the user interface of a system or device. Any interface that a user can interact with on a system to input or receive data is categorized under the user interface. A layout refers to the back-end set-up of how an interface would appear on a screen. There are different layout structure templates available on the Android Studio IDE. These Layout templates can be adopted directly or altered to fit the developer's design.

Figure 5 shows the front-end user interface and the back-end code layout and de-sign of the home interface of the SAPP application. The Home interface is the first interface a user is shown upon signing into the SAPP. Again, returning to the application after a closedown or a pause, the user will be shown this home interface.

B) Security UI and layout

The following user interface is the security activity interface. The interface uses a scrollable layout view that enables users to scroll through from top to bottom. The security activity interface contains a list of security and emergency parameters.

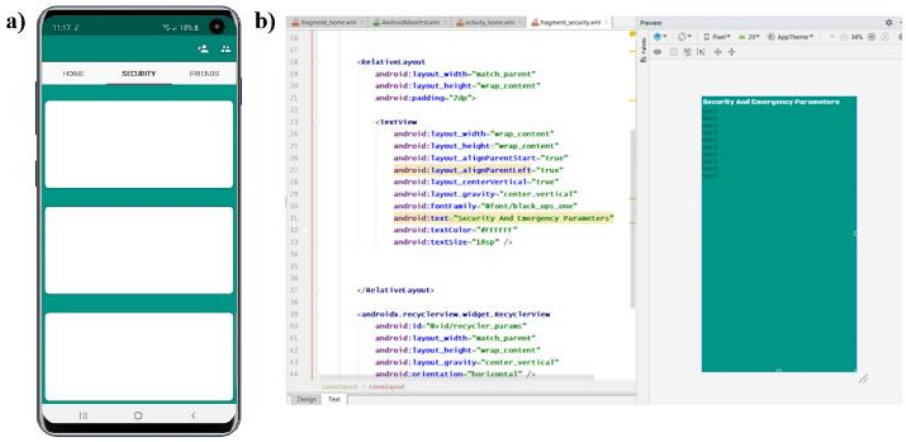

Figure 6. (a) Emulated security activity interface (b) Back-end code layout and design of security interface

The back-end layout design of the security activity was developed to accommodate-date the security and emergency parameters. An image button with a flexible width was added to contain the individual security and emergency parameters. On the back-end of the layout design, two types of layout preamble were used: Linear layout and Relative layout. The front-end interface and back-end design layout inter-faces are showcased in Figure 6.

C) Friends UI and layout

Figure 7. (a) Emulated friends' activity interface (b) Back-end code layout and design of friends' interface

The Friends user interface encompasses all the users' accepted friends and added friends on the SAPP. The back-end layout design on the android IDE that births the mobile UI for the friend's activity consist of an Android search widget that was added to enable the user to search for a friend on their friend lists. Figure 7 shows the emulated friend lists design layout and the back-end design and text mode development layout for the friend's activity fragment.

2.5 The Dynamics of SAPP Operation

The dynamics of the SAPP explain it's behind the scenes operations, rendering an understanding of the inner workings of the SAPP. It shows how it harmonizes major development components such as the Google Firebase services, android studio XML for layouts and

UI, Java main object library, Google Maps-API services, and Android OS classes to enable the SAPP mobile application function flawlessly.

A) Google Push Notifications and Security Alerts

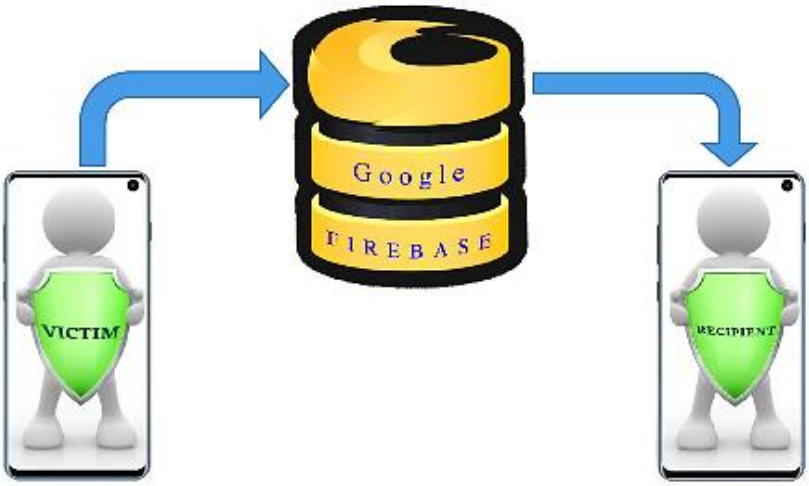

Figure 8. Firebase base acting as an intermediary between victim and recipient

The SAPP uses Google Cloud Messaging Services (CMS) for its emergency parameters, enabling push notifications on Android devices. In an emergency, SAPP captures the user's current GPS location and the selected emergency parameter, sending this data to Google Firebase database. Firebase identifies the victim's friends list and promptly sends distress alerts to their devices, taking under two seconds. If these recipients are online, they receive a notification. Clicking on it opens an embedded Google map in SAPP, pinpointing the victim's location. This can also link to third-party apps like Google Maps for navigation to the emergency spot. Similarly, chat and media functionalities utilize Firebase, which acts as the central hub for all messaging and notifications, as depicted in Figure 8.

B) Emergency Flow Process in SAPP

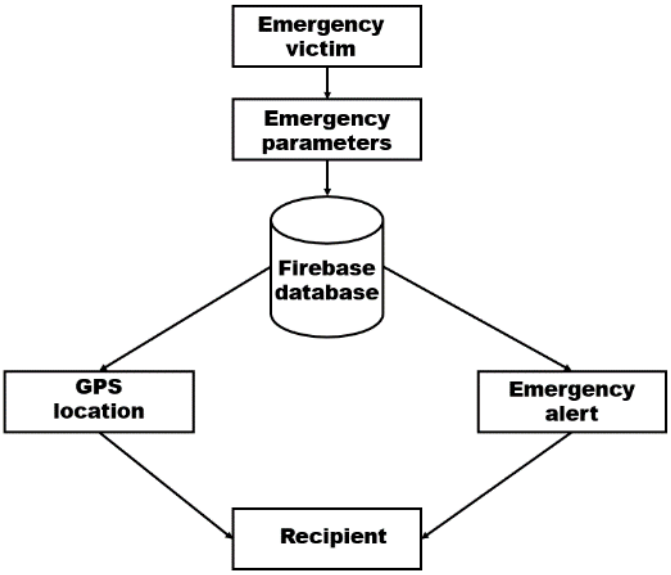

Figure 9. Proposed SAPP Flow of information

When a victim has an emergency that requires assistance, he/she activates the specific security parameter. The selected emergency parameter goes through the fire-base databases, which forwards the emergency alert and the victim's GPS location. Figure 9 shows the flow of events on the proposed SAPP application.

3.0 Results and Discussion

This section discusses the functionality and output of the various facets of the proposed SAPP application, involving features such as the initial user registration process, user interfaces (UI) and layouts, the security features, and the practical out-put of its utilization. Based on the SAPP design, any application user could perform three activity layouts: the home activity, security, and friend list functionalities.

3.1 User Authentication

The SAPP's user authentication integrates methods for signing in or up using the firebase database provided by Android Studio. Although Firebase offers various authentication processes, including Email, Phone number, Gmail, Pinterest, Twitter, and more, this study primarily utilizes Gmail and phone number. This choice is rooted in the ubiquity of phone numbers among mobile users and the prevalence of Gmail accounts, especially among Android users, given that Android OS is Google-owned. Moreover, statistics indicate that Gmail is the predominant email service, with a vast majority of users owning an account (Grevet et al., 2014; Khawas & Shah, 2018).

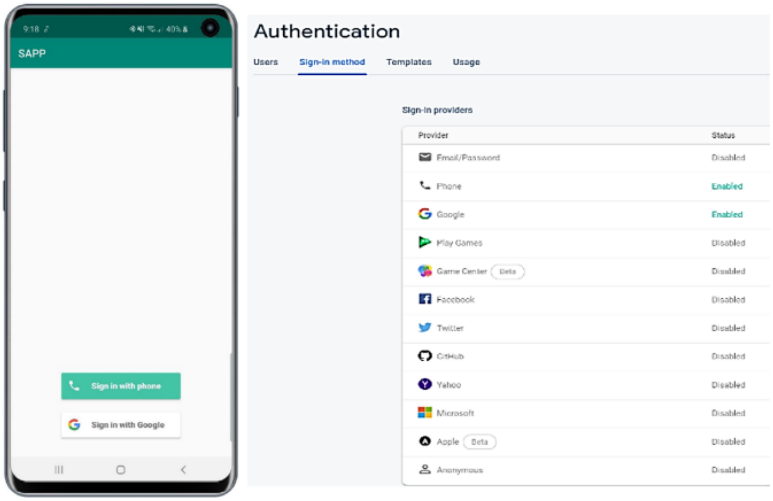

Figure 10. Proposed SAPP authentication options

Upon launching the App, users first encounter the authentication activity. Figure 10 highlights the available authentication options via the firebase database, with only two selected methods activated.

Figure 11. Home Interface of proposed SAPP

SAPP requires internet connectivity. Due to Android OS policies, apps must seek user permissions to access the internet, ensuring no unexpected high data usage. SAPP will ask for this permission during installation, essential for its notifications and tracking features.

After successful sign-in, the home activity displays the user's contact details and name, as well as guidance through unassigned image buttons. These include navigation tips and brief SAPP insights, with one dedicated for admin support contact. Figure 11 provides a visual of this home activity.

3.2 Security Activity

The security activity page in the application showcases a list of security and emergency parameters. Each parameter is represented with a humanoid 3D image for clear understanding, and in cases where such images aren't suitable, 2D images or icons are used. Eighteen security concerns, including accidents, childbirth, fire, floods, theft, kidnapping, and terrorism, among others, are featured. Additionally, an "other emergencies" option is included for situations not specifically listed. The layout of this security interface is depicted in Figure 12.

Figure 12. Security interface of proposed SAPP

3.3 Sending and Reception Emergency Concerns

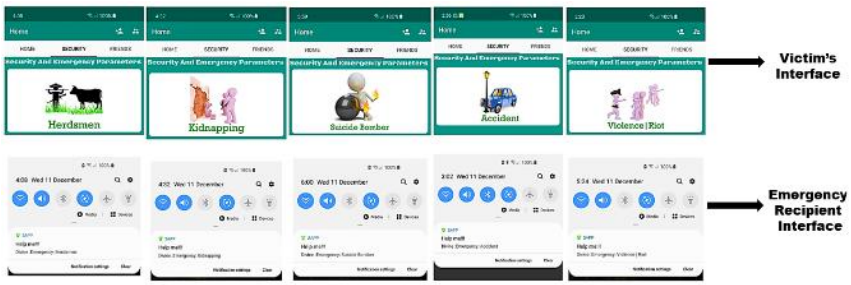

Figure 13. Victim's distress call options and emergency respondent received notifications.

Figure 14. Victims' real-time location on emergency respondent's smart device

Under the security activity section is the list of security parameters (i.e., 13 security and emergency concerns). When a user finds himself/herself in a troubling situation, he/she can activate any of the parameters of concern by clicking on it. Immediately, the security concern is transferred to all the contacts saved on the friend list. Hence, all the friends on the victim's friend list receive a pop-up notification on their smart devices informing them of the registered plight of their friend. The display of the security concern options for the victim and the recipient's pop-up notification is shown in Figure 13.

Upon clicking the pop-up notification, the emergency recipients can be navigated to the map activity, which shows the pinpoint location of their friend in trouble, as shown in Figure 14. After depicting the victim's location, the emergency contact could render the help he/she could or contact law enforcement agencies, depending on the situation.

4.0 Conclusion

In addressing Nigeria's significant security challenges, this study introduces the SAPP application, leveraging smartphone technology to enhance emergency response. SAPP's unique approach in providing real-time location data and alert mechanisms represents a shift from traditional security measures, emphasizing the potential of mobile technology in managing crises.

Comparatively, SAPP's tailored solution for Nigeria's security landscape showcases its distinctiveness from similar applications, indicating its potential for broader societal impact in improving community safety and aiding crime prevention. However, SAPP's current reliance on smartphone accessibility and internet connectivity is a notable limitation. Future iterations of the app should consider offline functionalities and gesture-based controls for initiating alerts in high-risk situations, enhancing usability and effectiveness.

Although it is an ongoing study, the research contributes significantly to the field of mobile security applications, with stakeholders ranging from emergency responders to the general public in Nigeria. These insights are invaluable, offering a framework for similar security challenges globally. To further refine SAPP and adapt it to user needs and security dynamics, empirical evaluations of its usability and effectiveness in real-world scenarios are recommended. Such studies will provide critical feedback, shaping future developments and ensuring the app's alignment with its intended purpose and user requirements.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

We would like to express our sincere gratitude to Ipsis (Institute of Post Graduate Studies), Universiti Teknologi Mara (UiTM), for their generous financial support, which made the publication of this manuscript in the conference proceedings possible. Their commitment to advancing academic research is truly commendable, and we are honored to have received their sponsorship.

References

Acheampong, R. A. (2021). Societal impacts of smart, digital platform mobility services—an em-pirical study and policy implications of passenger safety and security in ride-hailing. Case Studies on Transport Policy, 9(1), 302–314. https://doi.org/10.1016/j.cstp.2021.01.008

Adebakin, M. A. Raimi, L. (2012). National Security Challengesand Sustainable Economic Devel-opment: Evidence from Nigeria. Journal of Studies in Social Sciences ISSN 2201-4624 Vol-ume 1 (2012), Number 1, 1-30, 1(1), 1–30.

Adesoji, A. (2010). The Boko Haram uprising and Islamic revivalism in Nigeria. Africa Spectrum, 45(2), 95–108. https://doi.org/10.1177/000203971004500205

Afzal, M. (2020). From "Western education is forbidden" to the world's deadliest terrorist group. Foreign Policy at Brookings, April, 2–28.

Dah, J., & Hussin, N. (2021). A Conceptual Framework of a Streamlined Extended Technology Acceptance Model for Mobile Application Adoption. International Journal of Social Sci-ence Research, 9(2). https://doi.org/10.5296/ijssr.v9i2.18649

Giovanni, J. Di. (2014). The Deadly Mission of Boko Haram; The kidnapping of 276 Nigerian girls has put Islamist militants Boko Haram on the map. What do they want? Newsweek, 162(21). https://go.gale.com/ps/i.do?p=HRCA&sw=w&issn=00289604&v=2.1&it=r&id=GALE%7CA371931741&sid=googleScholar&linkaccess=fulltext

Global Terrorism Index. (2018). 2018 Global Terrorism Index. http://visionofhumanity.org/app/uploads/2019/01/GTI2018-A3-poster-wall-chart.pdf

Global Kidnapping Epidemic | LinkedIn. (n.d.). Retrieved August 30, 2022, from https://www.linkedin.com/pulse/global-kidnapping-epidemic-scott-bernstein/

Grevet, C., Choi, D., Kumar, D., & Gilbert, E. (2014). Overload is overloaded: Email in the age of gmail. Conference on Human Factors in Computing Systems - Proceedings, 793–802. https://doi.org/10.1145/2556288.2557013

James, A. (2013). A seminar report on Accident Detection and Reporting System using GPS , GPRS and GSM Technology Submitted by. IEEE/OSA/IAPR International Conference on Informatics, Electronics & Vision Accident, September 2013, 29.

Javale, D., Mohsin, Mohd., Nandanwar, S., & Shingate, M. (2013). Home automation and security system using IoT. International Journal of Electronics Communication and Computer Tech-nology, 3(2), 21–24. https://doi.org/10.18280/ria.330104

Khawas, C., & Shah, P. (2018). Application of Firebase in Android App Development-A Study. Article in International Journal of Computer Applications, 179(46), 975–8887. https://doi.org/10.5120/ijca2018917200

Lacatus, C., Akopian, D., & Shadaram, M. (2012). Reduced complexity crosscorrelation interfer-ence mitigation in GPS-enabled collaborative ad-hoc wireless networks - Theory. Computers and Electrical Engineering, 38(3), 603–615. https://doi.org/10.1016/j.compeleceng.2011.05.001

Miriyala, G. P., Sunil, P. V. V. N. D. P., Yadlapalli, R. S., Pasam, V. R. L., Kondapalli, T., & Miri-yala, A. (2016). Smart Intelligent Security System for Women. International Journal of Electronics and Communication Engineering & Technology (IJECET), 7(2), 41–46.

Moroney, L. (2017). The Firebase Realtime Database. The Definitive Guide to Firebase, 51–71. https://doi.org/10.1007/978-1-4842-2943-9_3
Nya. (2018). Kidnap for Ransom Global Trends 2017. April.

Qureshi, K. N., Naveed, A., Kashif, Y., & Jeon, G. (2021). Internet of Things for education: A smart and secure system for schools monitoring and alerting. Computers and Electrical En-gineering, 93(March), 107275. https://doi.org/10.1016/j.compeleceng.2021.107275

Ribeiro, A., Ferreira, J. F., & Mendes, A. (2021). EcoAndroid: An Android Studio Plugin for Developing Energy-Efficient Java Mobile Applications. IEEE International Conference on Software Quality, Reliability and Security, QRS, 2021-December, 62–69. https://doi.org/10.1109/QRS54544.2021.00017

Saigh, M. M., Kevin Richard Arndt, & Saigh, A. V. (2014). PERSONAL SAFETY MOBILE NOTIFICATION SYSTEM. United States Patent, 1–23.

Sheriff F. Folarin, P. (2014). Cultural Plurality, National Integration and The Security Dilemma In Nigeria. Covenant University Journal of Politics and International Affairs, 2(1), 81–92.

Singh, R. (2014). An Overview of Android Operating System and Its Security Features. Journal of Engineering Research and Applications Www.Ijera.Com, 4(2), 519–521. http://ptcoresec.eu/2013/05/02/part-1-getting

Sweidan, S. Z., Saifan, R., Darabkh, K. A., Abu-Kaff, S., & Al-Ali, S. (2017). Kids' Tracker: An Android Application for Tracking Children. Journal of Software Engineering and Applica-tions, 10(13), 907–924. https://doi.org/10.4236/jsea.2017.1013052

Varsha, S., & Srikanth, U. (2017). A Survey On Android Applications For Personal Security. International Journal of Modern Trends in Engineering & Research, 4(2), 1–7. https://doi.org/10.21884/ijmter.2017.4043.sgbkp

Vijayakumar, P., Pandiaraja, P., Karuppiah, M., & Jegatha Deborah, L. (2017). An efficient secure communication for healthcare system using wearable devices. Computers and Electrical Engineering, 63, 232–245. https://doi.org/10.1016/j.compeleceng.2017.04.014

Wu, D., Moody, G. D., Zhang, J., & Lowry, P. B. (2020). Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use in-tention. Information and Management, 57(5), 103235. https://doi.org/10.1016/j.im.2019.103235

Wu, S., Sun, W., Liu, X., & Zhang, Y. (2018). Forensics on twitter and wechat using a customised android emulator. 2018 IEEE 4th International Conference on Computer and Communica-tions, ICCC 2018, 602–608. https://doi.org/10.1109/COMPCOMM.2018.8781056

Yang, Q., Li, Z., Liu, Y., Long, H., Huang, Y., He, J., Xu, T., & Zhai, E. (2019). Mobile gaming on personal computers with direct android emulation. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM. https://doi.org/10.1145/3300061.3300122

Yarrabothu, R. S., & Thota, B. (2016). Abhaya: An Android App for the safety of women. 12th IEEE International Conference Electronics, Energy, Environment, Communication, Comput-er, Control: (E3-C3), INDICON 2015, 3–6. https://doi.org/10.1109/INDICON.2015.7443652

Yi, H., Qian, H., Yubin, W., & Zhiyong, X. (2014). Research on Global Positioning System in Mobile Communication Equipment Based on Android Platform. 888.