*Imaging and Radiation Research (2023) Volume 6 Issue 1*
doi: 10.24294/irr.v6i1.5411

ORIGINAL RESEARCH ARTICLE

# Mobile healthcare application on Android OS using cloud computing

**Nahla F. Omran**

*Faculty of Computers & Information, South Valley University, Qena 83511, Egypt; nahlaa.fathy@sci.svu.edu.eg*

## ABSTRACT

Healthcare mobile applications satisfy different aims by frequently exploiting the built-in features found in smart devices. The accessibility of cloud computing upgrades the extra room, whereby substances can be stored on external servers and obtained directly from mobile devices. In this study, we use cloud computing in the mobile healthcare model to reduce the waste of time in crisis healthcare once an accident occurs and the patient operates the application. Then, the mobile application determines the patient's location and allows him to book the closest medical center or expert in some crisis cases. Once the patient makes a reservation, he will request help from the medical center. This process includes pre-registering a patient online at a medical center to save time on patient registration. The E-Health model allows patients to review their data and the experiences of each specialist or medical center, book appointments, and seek medical advice.

***Keywords:*** cloud computing; healthcare; mobile cloud computing; android operating system; firebase

**ARTICLE INFO**

Received: 25 March 2023
Accepted: 6 May 2023
Available online: 30 May 2023



## 1. Introduction

One of the most significant developments is that the internet has enabled a vast number of items to be independently related and connected[1]. The use of information technology (IT) in the healthcare domain is largely untapped, especially in areas of operational efficiency. Most healthcare practitioners and institutions depend on paper medical records, restricting cooperation and coordination between patients and doctors. Cloud computing can help develop health services by providing information exchange between medical record systems and their users, patients, doctors, pharmacists, and all other geographically isolated centers and hospitals at any time. However, cloud computing faces challenges such as security and confidentiality, which have slowed its dependence on healthcare information management systems. Wearable fitness monitoring technology has been widely adopted during the past ten years as a result of the rise in demand for individualized health and home care, as demonstrated by products such as FitBit and Misfit[2].

Importantly, smartwatches enable user engagement, phone calls, and seamless connections with widely used cloud services, such as Amazon Web Services, AWS, and Microsoft Azure, in addition to facilitating fitness tracking[3,4]. Notably, these cloud services have forged alliances with reputable healthcare organizations[5,6], laying the groundwork for the fusion of fitness data from wearable devices with electronic health records (EHR). Healthcare professionals are actively investigating ways to connect the fitness data obtained from these devices with electronic health records, as wearable fitness technology has become more widely used by the general public. This integration

is particularly important in fragile and unsupervised elderly patients. Owing to declining motor function, these patients run the risk of suffering a decline in general well-being, increasing reliance, and a higher vulnerability to fall-related injuries. Noninvasive health monitoring tools offer significant advantages and are well-appreciated by patients for prolonged monitoring, particularly during the postoperative recovery phase[7,8].

This slowdown was caused by a lack of knowledge about whether the data were fully secure. In cloud computing, users often do not know where their data are stored or whether safety mechanisms are in place. Some patients need their medical information to be confidential and secure in order not to face social problems and to become subject to isolation, such as patients with HIV. Researchers argue that different security algorithms maintain the security of cloud data owing to encryption technology. An advanced encryption standard (AES) encryption system algorithm was used to encode text files and images[9]. A homogenous encryption method was also employed to protect the data from unwanted access[10]. Many encryption methods have been utilized to provide security to the data stored in the cloud. New generations of mobile devices offer clients better approaches to collaborate with increasingly expert medical systems in medical environments, such as emergency clinics, laboratories, hospitals, and intensive care units, to improve medical care and lessen the chance of settling on incorrect clinical choices[11]. The suggested model for mobile healthcare services employs Android handsets, including a server/client model connected to the Internet. A client is offered an appropriate front/end interface to use web service-based communication between the client and server. Every client has a user account on the E-Health mobile health system, and the supplied health services are accessible via various types of networks, such as 4G, 3G, Wi-Fi, and GPRS from far away, at home, or work.

In this paper, we presented E-Health, a new healthcare system that uses a cloud-computing server to store all information, records, and emergency healthcare services. The system helps clients locate the nearest medical center, view and recover information, for example, X-rays, obtain medical advice, reserve an appointment, and register at the hospital. It allows patients to review previous results and experiences with any doctor, matter expert, or medical center, allowing doctors to communicate with their patients more frequently and via mobile applications and exchange photos and messages of accidents or emergency cases.

## 2. Related work

Recently, there has been a marked increase in the smartphone adaptation process before healthcare professionals owing to the widespread and easy use of mobile devices. Many studies have been conducted because people worldwide are affected by various ailments. Mobile healthcare management solutions based on Android OS must be created to assist ordinary residents[12,13].

In this paper, we present the MADIP framework[14], which distributes information networks that enable mobile agent-based wide-area sharing of health information. However, most of these frameworks focus on costly and inflexible communication methods that require the mounting of software and hardware components. Using the principle of cloud computing, these problems were solved because there is no need for additional storage or computer media. Hospital management employees and doctors manage cloud-based details (prescriptions and medical imaging records can be uploaded). The Android OS upheld the cloud OS alliance that allowed patients, for example, HTTP URLs, to download, alter, track, and transfer clinical images and text information using Internet resources and other API concepts[14]. Image support was provided by the DICOM and Communications in Medicine protocol, and the JPEG standard compressed the pixel data of the images. In the study by Somasundaram et al.[15], the researchers created and developed the HMS application to be available on their Android-powered cell phones, medical picture records, medications, and health records (such as scanned images) of patients. The health records of the cloud OS were saved and handled. They were then transferred to the mobile device from the cloud where they were displayed. The application was developed using the EyeOS cloud platform. Because versatile mobile devices fueled by Android are accessible at reasonable rates, they may be effectively employed in similar healthcare software..

Vinutha et al.[16] developed cloud computing and an Android OS electronic hospital management system using VPN connections. By using a VPN, companies guarantee protection that cannot be read by someone intercepting encrypted data. The proposed system architecture presented by researchers for the creation and implementation of Cloud Computing and a VPN connection was used in an electronic hospital administration system application. In a study by Mallikarjuna[17], the completely atomic distributed environment of the Android operating system, which is popular in managing healthcare information used in cloud computing, a mobile healthcare application called HealthKit was developed. The proposed HealthKit framework consists of different cloud providers, the client running an Android OS application, and multiple modules, for example, clinic modules, patient health records, patient modules, cloud modules, and mobile device modules. Inupakutika et al.[18] introduced the Android HT Patient Helper prototype MHealth software to compare cloud-based and cloudlet-based versions of the app's results. For a data-intensive video retrieval test scenario, they conducted two evaluation campaigns for both versions and observed the Firebase cloud ( cloud -based) and cloudlet database (cloudlet-based) results. Nanda et al.[19] provided an EMS architecture using the MCC system, which offered important suggestions for people to save their lives during fires, floods, hurricanes, earthquakes, tsunamis, and other emergencies.

## 3. Research method

This section contains the structure of the proposed model, the software approach utilized to execute the study objectives, and the major circuit designs employed in the model. In addition, to compute the correctness of the proposed model, effective approaches were utilized to determine the accuracy and dependability of the data.

### 3.1. Software package

The app was designed using Google's Android software suite. Android is an open source model. The key programs, middleware, and operating systems are all included. The Android SDK includes libraries for communicating with high-level devices, as well as developing and publishing Android apps, Java apps, and Google's Firebase platform for storing persistent data. It has a ready-to-use infrastructure (back-end) that can be scaled-up (scalable). The back-end as a service platform is the name for this type of platform.

1) The Cloud Fire store is an NoSQL document database designed for easy application development, automated scalability, and excellent performance. Although the Firestore interface has many of the same capabilities as traditional databases, it varies in how it depicts connections between data items as a NoSQL database.
2) Cloud storage: Cloud storage aims to maintain data and files in an off-site location that can be accessed through the Internet or a private network connection. The data provided to third-party cloud services for storage have become their responsibility.
3) Authentication: Authentication is one of the most well-known and important services provided by Firebase. This mechanism is similar to the use of passwords in time-sharing systems for the secure authentication of network clients' identities by servers and vice versa, without assuming the operating system integrity of either party.
4) Cloud messaging: This service makes it easy for mobile application developers to set up a system to send alerts to user devices where the application is installed. Additionally, one can preview the data and analytics related to these alerts based on the users' behavior toward them.
5) Firebase hosting: A hosting service for static files, such as HTML, CSS, and JavaScript, in addition to other types of files provided through a known network for delivering content or acronym CDN via the secure HTTPS protocol.
6) Firebase remote configuration: A cloud service that enables developers to control and change the number of settings of their applications (configuration) without forcing users to update these applications on their

devices.

### 3.2. Method of research

Many other studies on mobile healthcare and cloud computing have been presented, but few successful papers and technologies have been executed in an effective system. Several Arab nations, such as the UAE, Bahrain, and Saudi Arabia, have developed mobile health applications that provide guidelines for keeping up with children, obesity, and heart diseases. Pregnancy and advertising of the vaccination season for children and babies have grown widely, but they do not have interactivity for communicating with specialists and physicians, and mobile medical records are not accessible to patients. In an emergency, patients employ Google services to identify the nearest medical center/specialist, receive a diagnosis, administer first assistance, and, if necessary, schedule appointments using a Global Positioning System (GPS).

The model concentrates on creating flexible mobile software to be used in an emergency to send user information to a medical facility, thereby saving time that would otherwise be lost via traditional techniques.

Three key components of the model were provided in this study.

1) The cloud computing system that houses emergency services as well as the database that is housed there.
2) There are three types of users.
3) In a structure (E-Health), the interaction is between mobile applications that allow the user to utilize emergency services.

The user's three levels are patient/ordinary user, specialist, and administrator. When the user starts the program, it detects the present position, allows the user to locate the nearest medical center, and requests assistance and emergency services. The request from the accident site and patient information are promptly sent to the cloud computing server.

### 3.3. Flowchart of the E-Health system

**Figure 1** shows a flowchart of the E-Health model. When the client launches the program, it is sent to a login screen. For registered users or those using the registration interface for the first time, the user selects the following types:

1) Patient user: The model detects the user's present position and then searches for the nearest specialist or medical center. It will then receive a list of administrations to display results and medical images, as well as the ability to make contact with an expert and set up an appointment.
2) Professional users: They will be contacted by credentials to log into the system and reply to requests to update their profiles, get messages, and schedule appointments.
3) System administrator: He/she is in controls all data in the system.
    (1) Specialists can be added, removed, or approved.
    (2) Medical centers/hospitals can be added or removed.
    (3) Database information can be maintained.

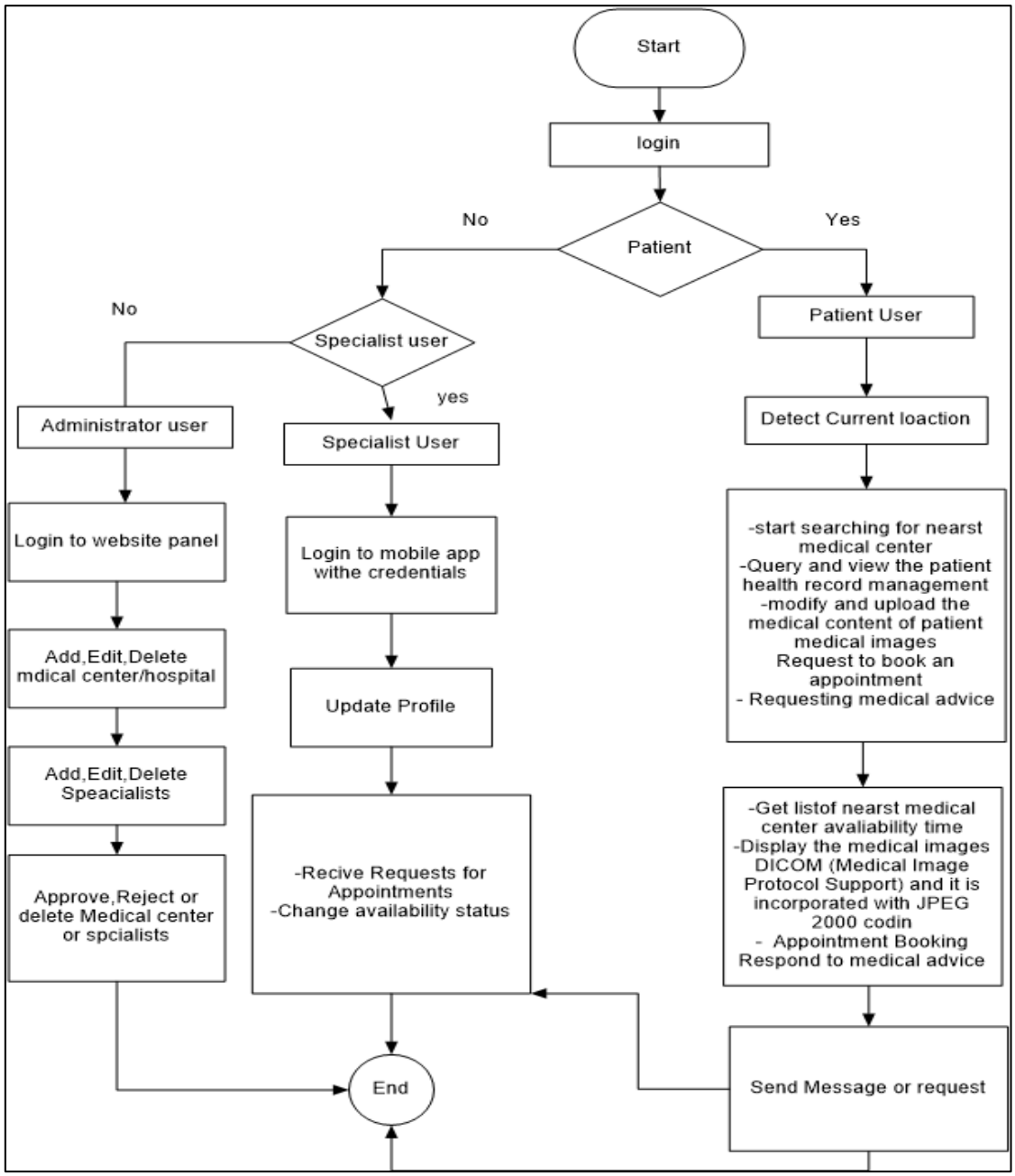



**Figure 1.** Flowchart of the E-Health system.

### 3.4. Architecture of the model

**Figure 2** illustrates the three key components of the e-health concept:

1) Medical Data Centers, Specialists, and Clinics: These entities are integrated into a centralized database managed via cloud computing. Medical images from various healthcare applications are stored using Firebase. Authenticated users access this system through a client-server architecture.
2) Web Services for Specialists, Medical Centers, and Patients: These services manage all data within the system and handle user requests such as authorizing new specialists, verifying profiles, and accepting or rejecting applications. Initial diagnostic sessions and patient help requests are processed within this cloud computing system, which retrieves and updates data from the database.
3) Mobile Healthcare Application for Customers: This component facilitates customer interaction with the healthcare system. Clinical users, such as medical centers, can use the mobile app, which is connected to online services to retrieve and submit data to the database.

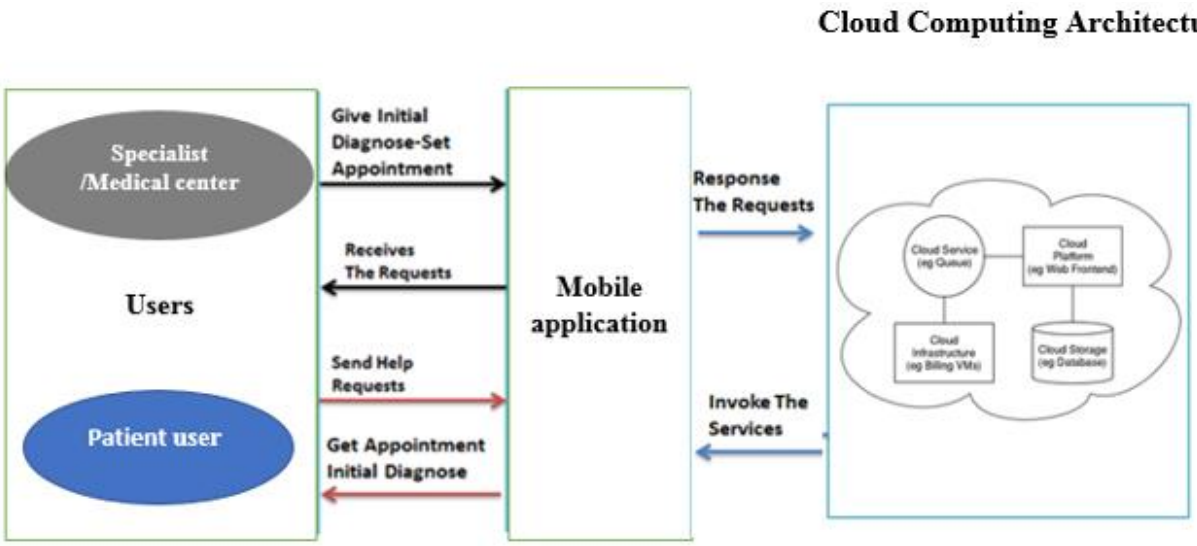



**Figure 2.** E-Health model architecture.

### 3.4.1. Cloud computing for E-Health

A shared pool of computer resources, such as servers, on-demand applications, and storage, is referred to as "cloud computing"[20]. Cloud computing offers low costs, great scalability, quick access to data records, high availability, and disaster recovery capabilities, making it an effective solution for addressing issues related to the storage and analysis of patients' medical records. This study examines the impact of cloud computing on enhancing healthcare services.

In the emergency healthcare sector, cloud computing provides unlimited capacity and processing power, enabling more specialized assistance to patients following accidents and before their arrival at medical facilities[21,22]. By pooling resources in the healthcare domain, cloud computing facilitates the efficient and exclusive use of machines. E-usage Health's cloud storage system benefits all treatment centers, consultants, and user information data by maintaining all emergency services in the cloud. These services are accessible on demand via mobile devices.

### 3.4.2. Users of E-Health

The device architecture in **Figure 1** shows two user categories:

1) Professional Users: Professional users who join the network or sign up will be able to use the mobile application to create a new account and receive approval or rejection from a system administrator.
   (1) Fill out their profile with personal information, geographical address details, and available hours.
   (2) Accept scheduling requests or notifications for appointments, if applicable.
2) Patient Users:
   (1) In the event of an accident, a patient can identify the nearest emergency center and schedule an ambulance.
   (2) If a health problem arises for a family member late at night, such as a toothache, fever, or other pain, the patient can locate the nearest available physician, enroll in the medical center/doctor, and schedule an appointment.
   (3) Using their current location and selecting from a set of professions (e.g., family dentists, physicians, gastroenterologists, neurologists), a patient can locate the appropriate healthcare provider, such as family dentists, doctors, neurologists, or gastroenterologists.

### 3.4.3. E-Health is a smartphone application

Certainly! Here's the text with grammar corrections and improvements for clarity:

The third component of the E-Health Architecture is the mobile application. This user-friendly mobile

cloud computing application enables users to locate nearby specialists or medical centers, send emergency requests, and schedule appointments. The process begins with an initial interface that asks whether the user is a patient or a specialist, as shown in **Figure 3**.

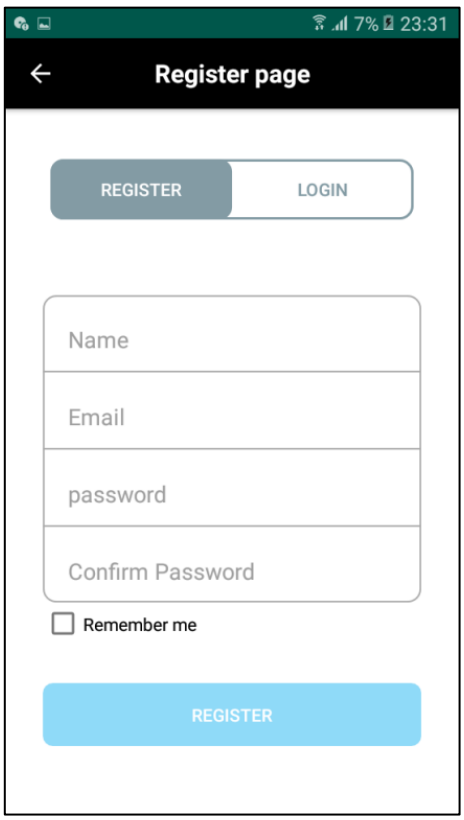



**Figure 3.** Registration interface.

When a user or patient selects the login button, the software detects their location and proceeds with the operation once the help request has been submitted, as seen in **Figure 4**.

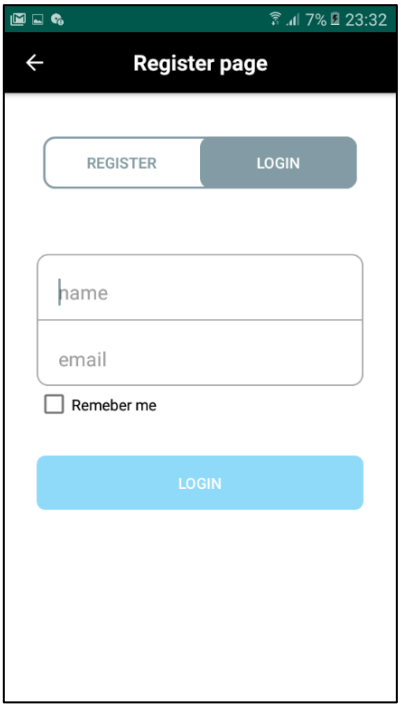



**Figure 4.** Login interface.

Certainly! Here's the text with improved grammar and clarity:

The user will then be asked if they are searching for an emergency at a medical facility or scheduling an appointment with a specialist. Next, the user can select a specialty and begin the search process, which should take no more than one minute. As illustrated in **Figure 5**, the user will receive the results on their mobile device.


**Figure 5.** Main interface.

"The user can contact the specialist through the interfaces shown in **Figures 6** and **7** to request medical advice or schedule an appointment, if necessary. The results are then communicated back to the user after review by the specialist. If the user is a technologist, they will be directed to the login/registration interface (see **Figure 4**). Upon completing the registration procedure, the specialist can access their account, update their profile, check messages, and respond to appointment requests. **Figure 8** demonstrates how users will be assisted during consultations, confirming dates, or rescheduling appointments by providing an interface displaying the relevant data. **Figure 9** accesses the interface to view, add, or delete doctors.

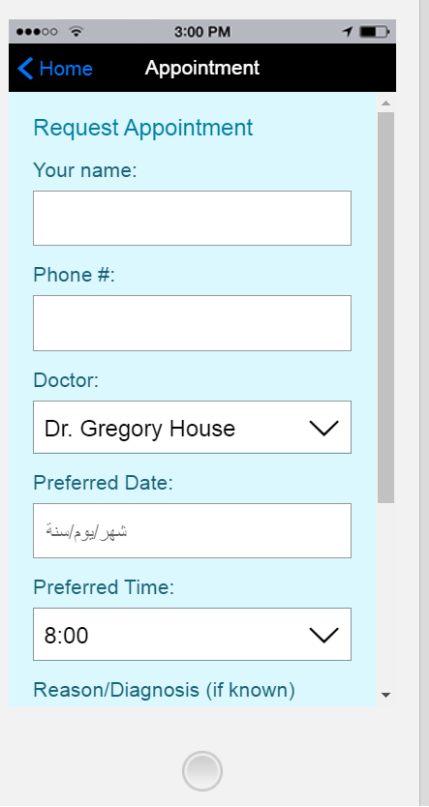



**Figure 6.** Interface of scheduling appointments.

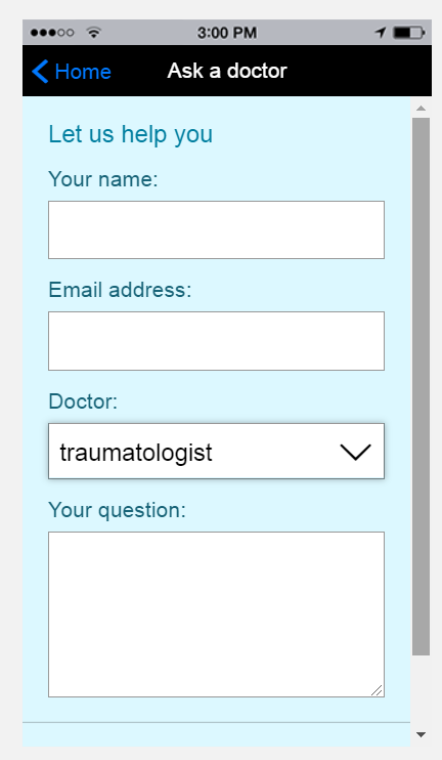



**Figure 7.** Interaction with the "Ask A Doctor" feature.

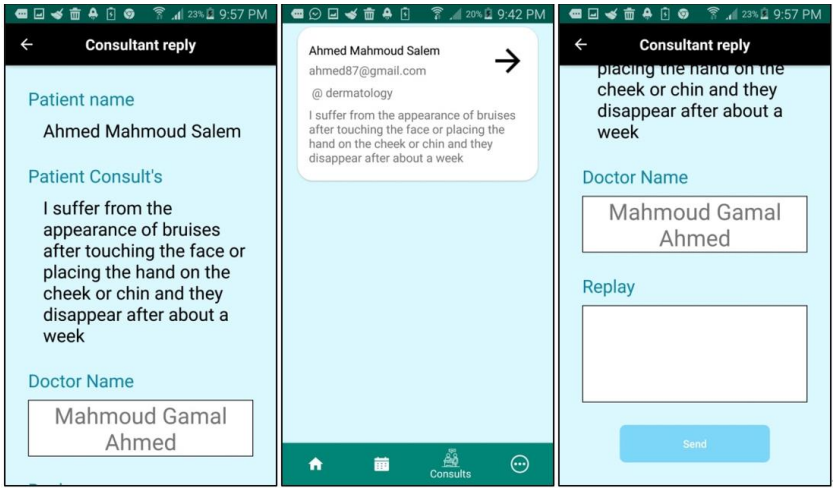



**Figure 8.** Make and reply to consultant interface.

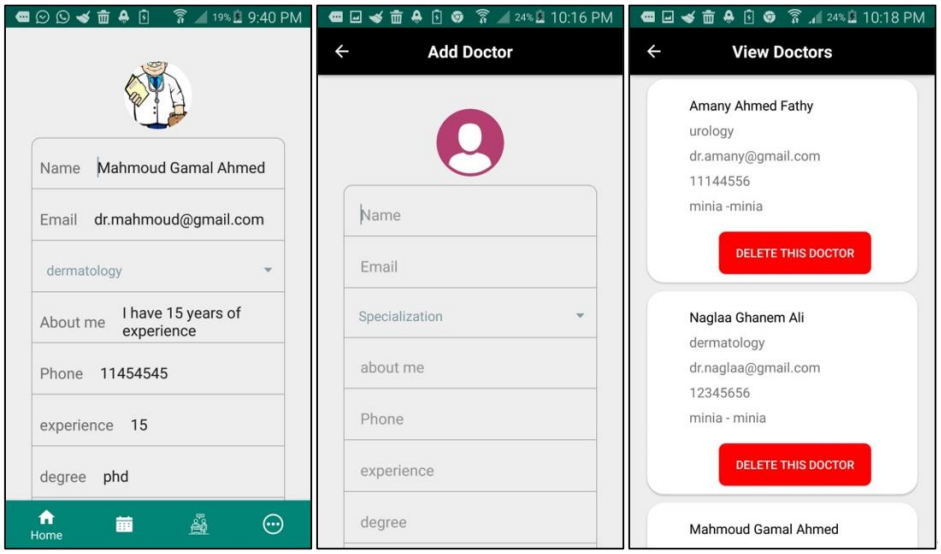



**Figure 9.** View, add or delete doctor interface.

### 3.4.4. Healthcare mobile system implementation

For patients and beneficiaries, the proposed paradigm involves utilizing mobile devices and applications connected to the Internet via wireless networks, facilitating connection to the cloud and utilizing the Firebase Cloud Platform[23,24] as a backend. Firebase is a free cloud service from Google that enables users to easily deploy applications on different platforms such as Windows, iOS, and Android[25,26]. The Infrastructure as a Service (IaaS) model and the platform are utilized to connect these applications directly to cloud databases operating in real-time on the Firebase platform.

Due to the challenges of offering such capabilities in Egyptian society, a simple prototype model was developed to provide basic services via mobile phones running on the Android system. This is achieved by downloading the health application linked and integrated with the Firebase cloud. Storage, editing, and data processing are handled by the Firebase cloud. This model serves as a basis for constructing a communication model, with the user's mobile phone acting as a lightweight client connected to the cloud. One of the mobile cloud computing concepts illustrated is the client-server model.

The application was developed entirely in Android Studio (refer to **Figure 10**) and subsequently connected to the Firebase platform as a cloud service using Java.

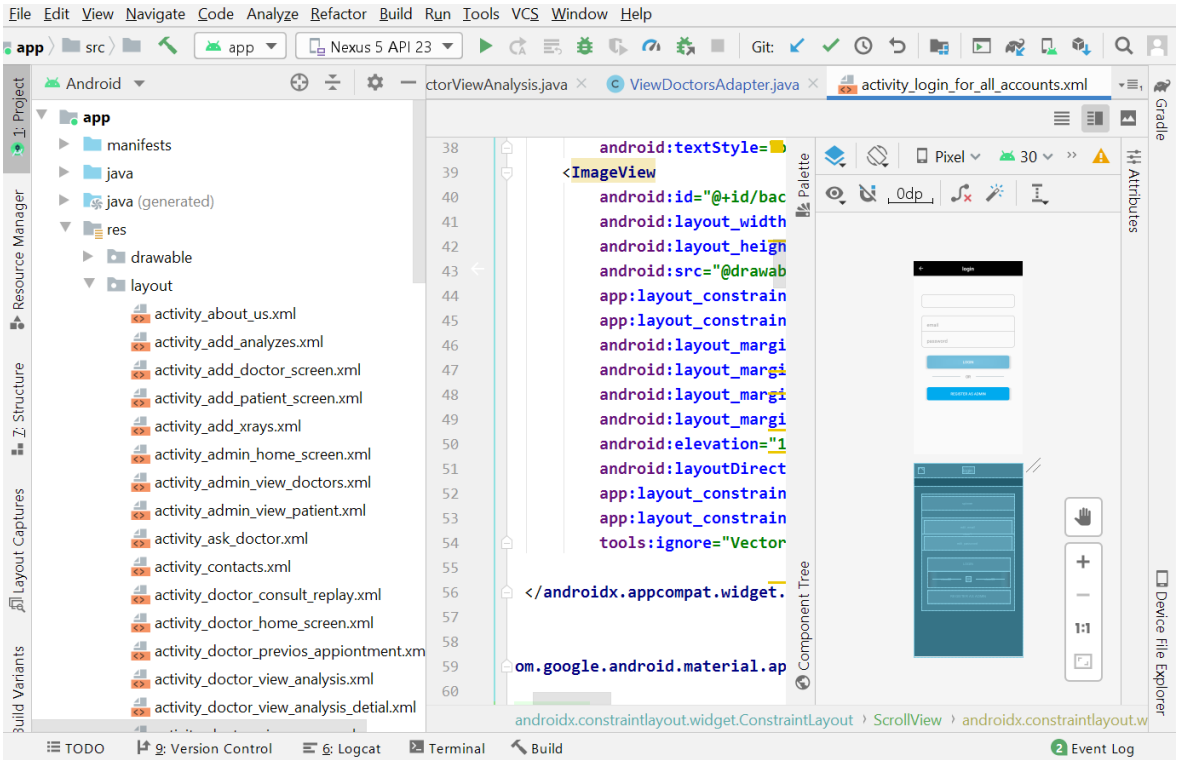



**Figure 10.** Android studio program layout.

**Figure 11** illustrates the real-time database, Firebase platform, and cloud services provided, along with the data stored in the database that users will access through the app.

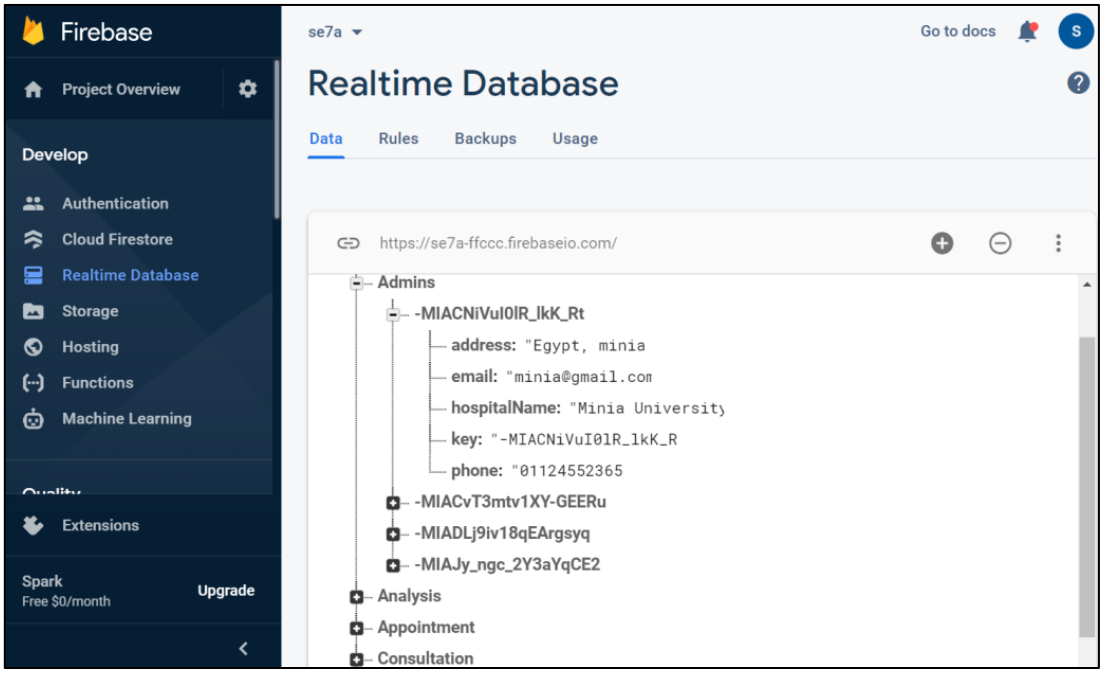



**Figure 11.** Firebase platform and services, and cloud database.

## 4. E-Health system security

Privacy and security are significant challenges in Mobile Cloud Computing (MCC) applications for healthcare. In this E-Health paper, we propose a secure architecture for mobile cloud services, ensuring the protection of E-Health apps through cloud security knowledge management. Users' mobile devices can securely communicate data in the cloud via the secured information service.

The suggested system comprises the following components:

1) Data Owners:

Patients with data stored in Electronic Health Records (EHRs) are considered data owners. As hospitals maintain patients' electronic healthcare data, patients need not expend money and time to provide their medical history when seeking treatment. Patients typically no longer require paper health notes since electronic health data are stored in the cloud. They may be shared with other healthcare facilities only with the patients' consent.

2) Electronic Medical Records:

Electronic Health Records are digitally recorded medical data containing patient information such as medical history, current medications, scan results, X-rays, and other sensitive information that must be kept private. EHRs may be stored in the cloud and updated and processed as needed, with physicians and authorized users having easy access to them. Various techniques have been established in EHRs as they may take the form of text or multimedia content, including photos.

3) Encrypted Communications:

The Advanced Encryption Standard (AES) technique is utilized to protect electronic health records. AES is a symmetric encryption method that encrypts and decrypts data using the same key, with a primary size of 128 bits for plaintext encryption. This method can encrypt both text and image data.

4) Encryption Key:

An encryption key is a randomly generated string of bits used to scramble and unscramble data. Algorithms are employed to create encryption keys, ensuring each one is random and unique. The longer the key, the more difficult the encryption algorithm is to crack. The encryption key is utilized to encrypt, decrypt, and perform all tasks.

5) Cloud Storage and Recovery:

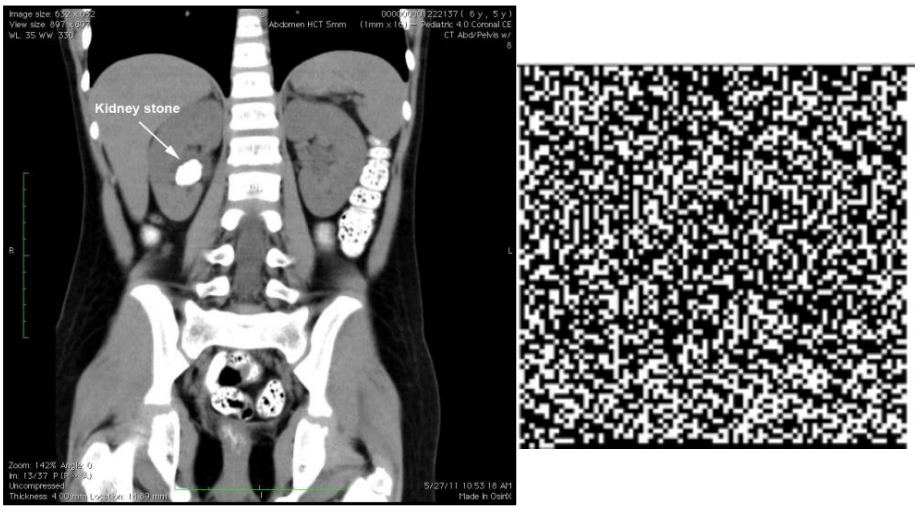
Encrypted files are stored in cloud data storage, providing customers with simple service expectations. Cloud data storage offers the infrastructure needed to store large amounts of electronic health data at a low cost. Cloud services are of high quality and well-suited to the healthcare industry, allowing physicians to easily access updated electronic healthcare records from the cloud whenever needed. Employing cloud services often reduces the time required to store and retrieve data. Electronic Health Records can be retrieved from the cloud and decrypted when combined with cipher messages.

6) Decryption:

Cloud-encrypted data are downloaded, and the decryption process is completed using a private key shared with physicians and other authorized users requiring healthcare information. The AES algorithm is used to generate the key, allowing text files to be decoded.

## 5. Results and analysis

The upcoming screenshots illustrate the original electronic health record alongside its encrypted version, as well as the provided encryption key and the resulting cipher texts generated from its use.




**(a)** **(b)**

**Figure 12. (a)** original health record; **(b)** encrypted health record.

**Figure 12a,b** presents the data before and after encryption, respectively. The plaintext electronic health record is displayed on the left, while the encrypted electronic health record (cipher text) is shown on the right. **Figure 13** The user-defined key grants access to the encrypted electronic health record.

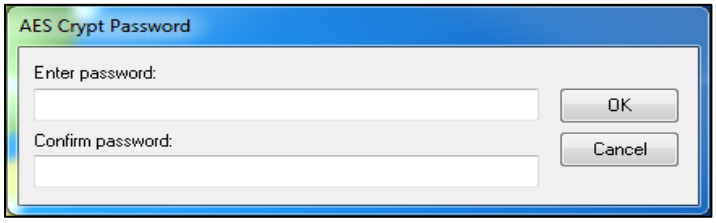



**Figure 13.** The key defined by the user to the encrypted electronic health record.

A test was conducted using a Samsung phone running Android version 10 to evaluate the readiness of the E-Health framework across various network types, such as 3G, 4G, and WLAN, as detailed in **Table 1**.

**Table 1.** How medical pictures were transmitted using the Firebase cloud service.

| Graphical style (encoding) | File size | Network 3G | Network 4G | Network WLAN |
|---|---|---|---|---|
| CT (uncompressed) | 0.530 MB | 1.57 | 1.22 | 1.2 |
| X-ray | 0.333 MB | 1.11 | 0.45 | 0.37 |
| MR | 0.733 MB | 2.40 | 1.50 | 1.22 |
| CT (JPEG 2000) | 0.110 MB | 22.0 | 0.018 | 0.11 |
| PET | 0.043 MB | 0.09 | 0.5 | 0.3 |
| Mammogram | 0.533 MB | 1.56 | 1.33 | 1.2 |
| Ultrasound | 0.498 MB | 1.47 | 1.33 | 0.50 |

The time taken to retrieve data from the Firebase Cloud service and transmit it to the E-Health application, as depicted in **Figure 14**, was measured.

Additionally, the impact of broadcasting medical images was investigated. These images encompass X-rays, a form of penetrating high-energy electromagnetic radiation, uncompressed computed tomography (CT) images, compressed CT images in JPEG 2000 format, Lossless JPEG images, positron emission tomography (PET) images in lossless JPEG 2000 format, ultrasound series consisting of ten images, and variously sized lossless JPEG 2000 images at different time intervals. The graph in **Figure 14** illustrates the successful

outcomes of the study.

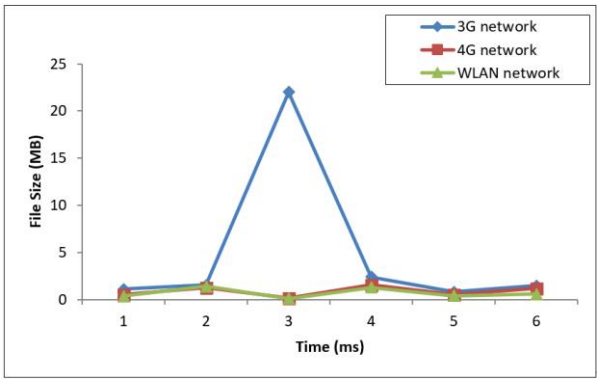



**Figure 14.** Effective result on WLAN.

## 6. Conclusion

The current healthcare system relies on paper records, often resulting in outdated prescriptions and ineffective medications being dispensed following health checks. Envisaging a shift towards a mobile healthcare system within a cloud computing environment tailored for the Android OS, the proposed E-Health application is poised to benefit a wide spectrum of users, including common folks, physicians, patients, and medical officials. It aims to streamline medical processes, including determining the appropriate medical equipment for patients. Leveraging advanced techniques on mobile devices such as speech recognition, along with innovative features like picture or video sharing through new IoT techniques, the system is set to evolve and expand its services. This evolution will lead to a diverse array of readily available services and applications.

## Conflict of interest

The author declares no conflict of interest.

## References

1. Hussien ZA, Jin H, Abduljabbar ZA, et al. Secure and efficient e-health scheme based on the Internet of Things. In: Proceedings of the 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). doi: 10.1109/icspcc.2016.7753621
2. Holko M, Litwin TR, Munoz F, et al. Wearable fitness tracker use in federally qualified health center patients: strategies to improve the health of all of us using digital health devices. NPJ Digital Medicine. 2022; 5(1). doi: 10.1038/s41746-022-00593-x
3. Hrad J, Vojtech L, Cihlar M, et al. Indoor Positioning System Based on Fuzzy Logic and WLAN Infrastructure. Sensors. 2020; 20(16): 4490. doi: 10.3390/s20164490
4. Azure Cloud Services. Available online: https://azure.microsoft.com (accessed on 18 October 2021).
5. Amazon's AWS Success Case Studies. Available online: https://aws.amazon.com/solutions/case-studies (accessed on 18 October 2021).
6. Microsoft's Azure Success Case Studies. Available online: https://azure.microsoft.com/en-us/case-studies (accessed on 18 October 2021).
7. Murphy J, Uttamlal T, Schmidtke KA, et al. Tracking physical activity using smart phone apps: assessing the ability of a current app and systematically collecting patient recommendations for future development. BMC Medical Informatics and Decision Making. 2020; 20(1). doi: 10.1186/s12911-020-1025-3
8. Ramezani R, Zhang W, Roberts P, et al. Physical Activity Behavior of Patients at a Skilled Nursing Facility: Longitudinal Cohort Study. JMIR mHealth and uHealth. 2022; 10(5): e23887. doi: 10.2196/23887
9. Aruna Devi S, Manju A. Enhancing security features in cloud computing for healthcare using cipher and inter cloud. International Journal of Research in Engineering and Technology. 2014; 3(3): 200-203. doi: 10.15623/ijret.2014.0303036
10. Ramakrishnan N, Sreerekha B. Enhancing Security of personal health records in Cloud Computing by Encryption. International Journal of Science and Research (IJSR). 2015; 4(4): 298-302.

11. George R. Cloud Application Architectures: Building George Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly Media; 2009.
12. Laxmaiah II, Meshram. Socio-economic & demographic determinants of hypertension & knowledge, practices & risk behaviour of tribals in India. Division of Community Studies, National Institute of Nutrition (ICMR), Hyderabad, India, Indian J. Med. Res.; 2015. pp. 697-708.
13. WHO. Publication Data Global status report on noncommunicable diseases 2010. WHO Library; 2011.
14. Doukas C, Pliakas T, Maglogiannis I. Mobile healthcare information management utilizing Cloud Computing and Android OS. In: Proceedings of the 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology. doi: 10.1109/iembs.2010.5628061
15. Somasundaram M, Gitanjali S, Govardhani T, et al. Medical image data management system in mobile cloudcomputing environment. In: Proc. Int. Conf. Signal, Image Process. Appl. (ICSIPA); Kuala Lumpur, Malaysia. 2011. pp. 11–15.
16. Vinutha S, Raju C, Siddappa M. Development of Electronic Hospital Management System utilizing Cloud Computing and Android OS using VPN connectionsl. International Journal Of Scientific & Technology Research. 2012; 1(6): 59-61.
17. Mallikarjuna B. Mobile Healthcare Application Development on Android OS in Cloud Computing. SSRN Electronic Journal. 2018; 93-100.
18. Inupakutika D, Akopian D, Chalela P, et al. Performance analysis of Mobile Cloud Computing Architectures for mHealth app. Electronic Imaging. 2020; 32(3): 335-1-335-337. doi: 10.2352/issn.2470-1173.2020.3.mobmu-335
19. Nanda S, Panigrahi CR, Pati B. Emergency management systems using mobile cloud computing: A survey. International Journal of Communication Systems. 2020; 36(12). doi: 10.1002/dac.4619
20. Kumar PR, Raj PH, Jelciana P. Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science. 2018; 125: 691-697. doi: 10.1016/j.procs.2017.12.089
21. Almorsy M, Grundy J, Müller I. An analysis of the cloud computing security problem. arXiv. 2016; arXiv:1609.01107.
22. Hanen J, Kechaou Z, Ayed MB. An enhanced healthcare system in mobile cloud computing environment. Vietnam Journal of Computer Science. 2016; 3(4): 267-277. doi: 10.1007/s40595-016-0076-y
23. Dinh HT, Lee C, Niyato D, et al. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing. 2011; 13(18): 1587-1611. doi: 10.1002/wcm.1203
24. Gunawan TS, Mutholib A, Kartiwi M. Design of Automatic Number Plate Recognition on Android Smartphone Platform. Indonesian Journal of Electrical Engineering and Computer Science. 2017; 5(1): 99. doi: 10.11591/ijeecs.v5.i1.pp99-108
25. Griffith C. Mobile App Development with Ionic, Revised Edition: Cross-Platform Apps with Ionic, Angular, and Cordova. O'Reilly Media, Inc.; 2017.
26. Vatika S, Meenu D. SQL and NoSQL Databases. International Journal of Advanced Research in Computer Science and Software Engineering. 2012; 2(8).
27. Varsha BS, Suryateja PS. Using Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud. International Journal of Computer Science and Information Technologies (IJCSIT). 2014; 5(6).