Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

An Advanced Encryption Standard (AES) Algorithm for Internet of Things in Telemedicine Practices

Andenwu Rimamskep Tanko
(Computing and Artificial Intelligence)
Taraba State University Jalingo, Nigeria

Doris Jonah Kyado
(Computing and Artificial Intelligence)
Taraba State University Jalingo, Nigeria

Ahmed Musa Iliyasu
(Computing and Artificial Intelligence)
Taraba State University Jalingo, Nigeria

Kamak Yamilach Shedrach
(Computing and Artificial Intelligence)
Taraba State University Jalingo, Nigeria

Maiyaki David Manasseh
(Computing and Artificial Intelligence)
Taraba State University Jalingo, Nigeria

Abstract

In this present dispensation, technology has turn the world into a global village. The internet has found a way to eliminate geographical boundaries between a patient and a doctor. Internet of Things (IoTs) working together with telemedicine has made remote diagnosis and treatment of patients possible. It plays a vital role in consultation and monitoring of patient's health. Due to the limitation of the generic web-based application in areas of granting easy access to information, and lack of secure database, the need for a standalone (Android) system and a secure cloud storage database becomes necessary. The research aimed at developing an encrypted android application using Internet of Things technology to carry out telemedicine services and providing a secured cloud storage. The methodology used in designing this system is Object Oriented Analysis Model. Health technologies such as telemedicine render a plethora of possibilities that can improve affordability, accessibility, availability, and quality healthcare services. The developed system, which is an android application, configured towards using the camera on an android device to take pulse reading of the patient, which will help to determine whether the patient's heart condition is normal or abnormal. A web based application developed to be used by the admin for registering of doctors, assigning doctors to patients, fixing consultation sessions between doctors and patients and monitoring the cloud storage.

Advanced Encryption, Standard Algorithm, Cloud-computing, Cryptography, Telemedicine

INTRODUCTION

The expression “Internet of Things” (IoT), coined back in 1999 by Kevin Ashton, the British technology pioneer who cofounded the Auto-ID Center at the Massachusetts Institute of Technology, MIT, is becoming more and more mainstream. What you see in present day is more and more objects become connected. If you are selling products, you will be negotiating with providers of connectivity. If you are building, selling or inventing models or tools for providing services or applications, you will notice the convergence of IoT, big data and energy efficiency, combined with cheap hardware, software, data storage and analytics, favors open standards, innovation and interoperability. Thus, in effect, the Internet of Things is a combination of a technological push and a human pull for more and ever-increasing connectivity with anything happening in the immediate and wider environment – a logical extension of the computing power in a single machine to the environment: the environment as an interface. This push-pull combination makes it very strong, unstoppable, fast and extremely disruptive (Kramp et al., 2013). Internet of things (IoTs) has evolved to become one of the most promising technologies in the industry and academics for innovation. The IoT devices will play a significant role in monitoring the health of patients. Telemedicine services are still in a developing stage in Nigeria. The remote diagnosis and treatment of patients by means of telecommunications technology has proven effective since its abduction into the healthcare system. Due to the lack of adequate/good doctors in rural and urban areas, healthcare services are not as good as it should be for consulting and monitoring of patient's health (Rolim et al., 2010). Therefore, the need of telemedicine sets in to cope with the situation. In the year 2020, the population of Nigerians living in rural areas reported at 48.04%. Due to lack of adequate/good doctors and lack of finance by the settlers in rural areas, death may become the fate of a patient suffering from an ailment.

On the other hand, in the urban areas, developed or in developing phase, where Internet services are readily available, many healthcare portals are accessible where Internet of Things (IoT) devices are supportive in healthcare services (Rolim et al., 2010).

A doctor using sensors and IoTs devices can monitor the health condition of a patient.

IoTs and E-health centers its attention on control and prevention, which are the two main goals Cloud computing helps in organizing the medical record at different levels of healthcare setting. Cloud computing is a promising and emerging technology for the users of the healthcare ecosystem by connecting many health information management systems together with laboratory, pharmacy, radiology and so forth. The main obstacles and serious problem towards the rapid growth of cloud computing are data security and privacy issues. Most of the healthcare users of private cloud do not fully trust the inside threat of the healthcare organization for safeguarding sensitive health information data because there is no governance about how this information can be used by them and whether the healthcare organization actually control their information. Healthcare management has become important due to the rapid growth of world’s population. Developed countries have been facing the trend of population aging, escalating costs, inconsistent provision of care, and a high burden of chronic diseases related to health behaviors. This situation makes healthcare management more and more important to all types of healthcare organizations. Health care is been delivered mainly through Primary Healthcare Centre (PHC), Secondary Care Centre (SHC), and Tertiary Care Centre (THC). The primary healthcare centre deal with patients whose medical conditions can be manage on an outpatient basis. The secondary healthcare usually deals with acute care hospitals whereas tertiary care requires the resources of a sophisticated medical center. Healthcare ecosystem consists of physicians, nurse, pharmacist, radiologist, lab technician, and patient (Ganiga et al., 2018).

Cryptography is a mechanism that ensures message confidentiality by eliminating an unauthorized user from understanding the message. Only the recipient can understand the message by first converting the message into its original form. Procedures like encoding and decoding needed to establish a cryptographic process. The original text called plain text while the encoded text called cipher text and the process of converting a plain text into cipher text known as encoding or enciphering and from cipher text to plain text called decoding or deciphering (Abdullah, & Aziz, 2016).

Cloud computing helps in organizing the medical record at different levels of healthcare setting. Cloud computing is a promising and emerging technology for the users of the healthcare ecosystem by connecting many health information management systems together with laboratory, pharmacy, radiology and so forth. The main obstacles and serious problem towards the rapid growth of cloud computing are data security and privacy issues. Most of the healthcare users of private cloud do not fully trust the inside threat of the healthcare organization for safeguarding sensitive health information data because there is no governance about how this information can be used by them and whether the healthcare organization actually control their information. Healthcare management has become important due to the rapid growth of world’s population. Developed countries have been facing the trend of population aging, escalating costs, inconsistent provision of care, and a high burden of chronic diseases related to health behaviors. This situation makes healthcare management more and more important to all types of healthcare organizations. Health care is been delivered mainly through Primary Healthcare Centre (PHC), Secondary Care Centre (SHC), and Tertiary Care Centre (THC). The primary healthcare centre deal with patients whose medical conditions can be manage on an outpatient basis. The secondary healthcare usually deals with acute care hospitals whereas tertiary care requires the resources of a sophisticated medical center. Healthcare ecosystem consists of physicians, nurse, pharmacist, radiologist, lab technician, and patient (Ganiga et al., 2018). Cryptography is a mechanism that ensures message confidentiality by eliminating an unauthorized user from understanding the message. Only the recipient can understand the message by first converting the message into its original form. Procedures like encoding and decoding needed to establish a cryptographic process. The original text called plain text while the encoded text called cipher text and the process of converting a plain text into cipher text known as encoding or enciphering and from cipher text to plain text called decoding or deciphering (Abdullah, & Aziz, 2016).

World Health Organization (WHO) defines telemedicine as the delivery of healthcare services at a distance using electronic means for ailment diagnosis, prevention, and treatment of illnesses. Gogia (2020) describe telemedicine as remote clinical services in the form of patient and clinician contact that covers diagnosis, advice, reminders, intervention and remote admissions. Telemedicine can be divided in to two words; Tele refers to the use modern communication scheme like wireless networks, and medicine, which is diagnosing a patient for any diseases and check patient’s wellness (Mohammad & Abdellatif, 2019). Smart phones notification are interruptive when delivered with little or no regard for the consumer’s (user’s) context – whether they are doing sports or attending an important meeting (Stothart et al,, 2015). This will ensure that a patient does not miss doctor’s appointment or time to take medication.

IoT is a large network comprising of devices connected to it (Krishna, 2020). The connected devices source data and show how they operate and perform specific tasks (Sahni et al., 2017). An IoT network comprises of web-enabled smart devices that use incorporated systems such as processors, sensors and communication hardware, to gather, transfer and act on data obtain (Medhat *et al.*, 2019). All IoT applications need to have at least one sensor to gather information from nature (de Cleber et al., 2019). A cell phone is a convenient easy-to-use device that has a large group of inherent correspondence and information preparing headlights. With the everyday growing prominence of cell phones among people, scientists have more interest in it due to the installed sensors (Khelifi et al., 2019). Applications can be based on cell phone that utilizes sensor information to deliver significant outcomes (Andrews et al., 2019). Review of Related Works

Ganiga et al. (2018) presented a security model to ensure safe storage and retrieval of sensitive personal information of patients. The model consists of central health record server in communication with a medical record repository or database stored on a remote system. The system makes use of two databases one for medical record and another for biometric information. Medical record database need not include personal identification of the patient (patient name) instead patient identification or biometric information is stored in the biometric database. Patient health information stored in the medical records may be identify using one or more identifier associated with the patient. Both the database are associated or linked using an alphanumeric pass-code. Using this pass-code medical record can cross-reference with biometrics data. The patient data are available for the patient without using the patient’s name or other personal information. The virtual machine in the private cloud consists of databases to store the patient data. Private cloud infrastructure provides compute, storage and network services for managing the data. In the dual database, to store the patient health information,

Electronic Health Record (EHR) database is used, in which data is stored in encrypted format. To store the key and hash value another database is used called key database. The main role is to perform encryption operation. In order to identify the key used for encrypting the data, the timestamp at which the operation was performed is also stored in the corresponding databases. Before storing data into the database, encryption is applied at the gateway to maintain confidentiality of the patient data. Therefore, the system uses key encryption for data security.

Sidorov and Keong (2015) proposed an approach to Transparent Data Encryption (TDE), which takes into account cloud-specific risks, extends encryption to cover data-in-use and partly datain-motion, and is capable of executing large subsets of SQL including relational operations, complex operations over attributes, and transactions. In the work, flexible and extensible abstract model is been used. The two types of entities used in the model are fully trusted and fully untrusted. The model presented tends to lower the probability and the adversary will obtain any plaintext data in a reasonable time to negligible levels. The proposed model by the authors acts as an agent between the user or the user-invoked application, and the remote relational database management system. The user need not to adjust his queries and may not be aware that the database is encrypted; thus, transparent data encryption. The model consists of three main parts namely; the Database Management System (DBMS) that runs on untrusted cloud platform, the user and the proxy. The proxy is a fully trusted intermediary agent between the user and the DBMS, who intercepts the plaintext queries from the user and transform them into encryption-aware queries with the same semantics. TDE is considering not being end-toend encryption solution for data. Some disadvantages of TDE is that master database which contains various metadata, user data and server level information cannot be encrypted, can only encrypt data at rest, can't reduce the size of a database therefore, makes it heavy as a result of compression, and so forth.

Hidayat and Mahardiko (2020) discussed on Advanced Encryption Standard (AES) algorithm that will serve as an approach to boost system security during data transfer and prevent data theft by unauthorized persons. The algorithm is meant to secure not just data transmission but also to data storage in cloud computing. The proposed encryption algorithm by the authors involves symmetric cryptographic called key to do the encryption and decryption. They made use of Systematic Literature Review (SLR) method to carry out the research. The Systematic Literature Review (SLR) has three steps. These are to plan review process, to do review process and to report review process. Authors utilize three digital libraries named "Science Direct", "IEEE Explore" and "Tandfonline" to source for data.

RESEARCH GAP AND REMARKS

From the related works reviewed above, it was discovered that the work of Narendra et al. (2020) has its system cloud based and had no facility to secure the storage of patients data in order to ensure data integrity and confidentiality. In addition, the web based software accessing time is high due to the many processes you have to undergo. Raghavendra et al. (2018) model lack cryptographic algorithm and entity authentication system to ensure data and system security. This proposed technique will eliminate some steps when accessing the software thus, increasing the system's access speed. The system will be integrated with a cryptographic algorithm and also an entity authentication system to further increase the security.

METHODOLOGY ADOPTED

The proposed system will make use of a standalone (Android) application to carryout telemedicine practices. The system will grant easy and fast access to information needed by either the doctor or patient, send instant notifications to its users, create a convenient user interface, provide an offline user mode and most especially ensure data security through data encryption. System model of the proposed system can be found in figure 3.3.

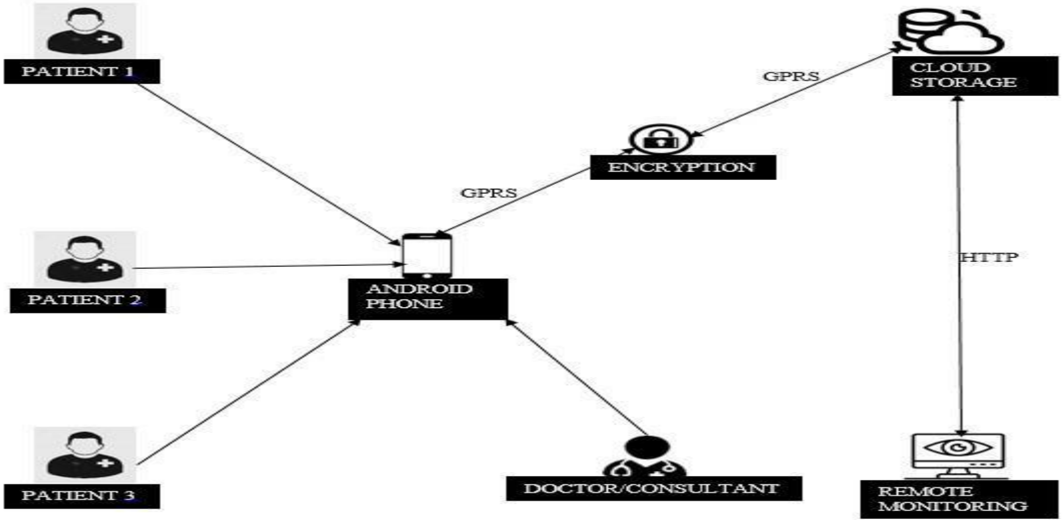


Figure 3.1. Model for Android-based Telemedicine Services.

Based on figure 3.3, we can explain the flow of telemedicine services as follows:

The patient checks the health condition at home using a bio-signal sensor device (android phone).
The data gotten on the device are transmitted through an internet data communication network.
Through the existing data communication network, data is transmitted to the server for processing (encryption) and storage.
Doctor/consultant can communicate with the patient, store and access data stored on the cloud server.
Data stored on the server can be accessed and monitored remotely by the hospital.

ENCRYPTION STANDARD (AES) ALGORITHM

The technique of this advanced algorithm was revealed by the National Institute of Standards and Technology (NIST) in 2001 (Islam, and Riyas 2017). AES is a symmetric block cipher by which DES is intended to be replaced. The Advanced Encryption Standard (AES) is a symmetric-key cryptographic technique dependent on substitution-permutation operations and that is so much fast in both sectors like software and hardware. AES doesn't use a Feistel cipher network like DES. It has two parts. One part is cipher key and another one is plaintext. The key length of the text can either be 128,192 and 256 bits. Its fixed block size like of 128bits or 16 bytes and key size 128, 192, and 256 bits. The cipher takes N rounds depending on the original length: 10 rounds for the 128-bit key, 12 rounds for the 192- bit key and 14 rounds for the 256bit key (Akhil, Praveen & Pushpa 2017; Lee, Dewi & Wajdi 2018). A round consist of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it in to the final ciphertext.

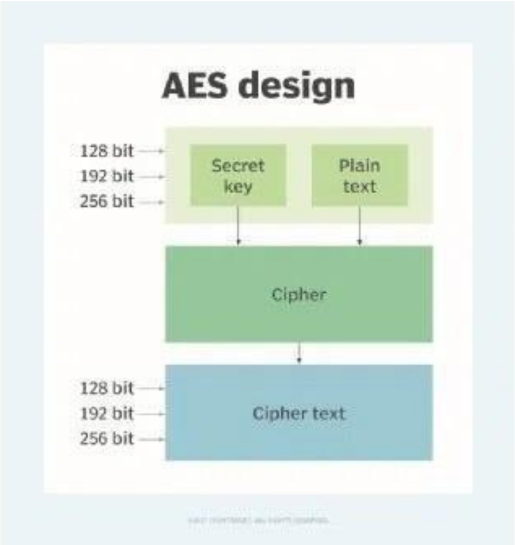
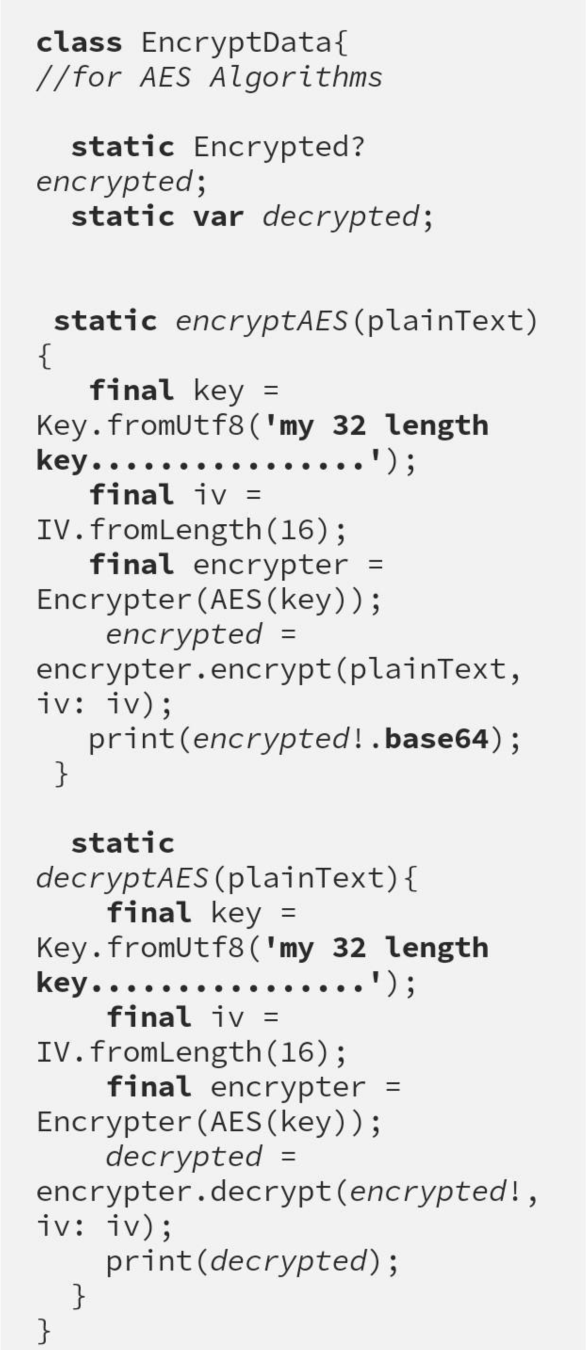


Figure 3.2. AES Design

The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data in to an array, after which the cipher transformations are repeated over multiple rounds. The first transformation in the AES encryption cipher is substitution of data using substitution table. The second transformation shifts data rows. The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to compete (Corinne, 2021).
The implementation of AES algorithm in an Android application developed in Flutter using Dart programming language can be seen showing methods of encrypting and decrypting.



```
class EncryptData{
//for AES Algorithms

  static Encrypted?
encrypted;
  static var decrypted;


 static encryptAES(plainText)
{
   final key =
Key.fromUtf8('my 32 length
key................');
   final iv =
IV.fromLength(16);
   final encrypter =
Encrypter(AES(key));
    encrypted =
encrypter.encrypt(plainText,
iv: iv);
   print(encrypted!.base64);
 }

  static
decryptAES(plainText){
    final key =
Key.fromUtf8('my 32 length
key................');
    final iv =
IV.fromLength(16);
    final encrypter =
Encrypter(AES(key));
    decrypted =
encrypter.decrypt(encrypted!,
iv: iv);
    print(decrypted);
  }
}
```

Figure 3.3. Method of Encrypting and Decrypting Data using AES Algorithm

Photo-plethysmography

Photo-plethysmography (PPG) is a non-invasive optical technique for detecting microvascular blood volume changes in tissues. Making use of fast digital cameras on phones for clinical image monitoring and diagnosis has inspired the evolution of conventional PPG technology to imaging PPG (IPPG). IPPG is a noncontact method that can detect heart generated pulse. (Sun & Thakor, 2015).

In respect to this work, we will concentrate on the noncontact IPPG technique, which is a noninvasive optical method for sensing the blood volume pulse, and it has been proven superior in its ease of use, low cost, safety, convenience, and ability to offer multiple physiological assessments.

HOW THE TECHNOLOGY WORK

As an optical technique, PPG requires a light source and a photo detector to function. The light source illuminates the tissue, and the photo detector senses the small variations in reflected or transmitted light intensity associated with changes in perfusion in the catchment volume. There are two main PPG operational configurations, the transmission and reflection modes, that depend on the geometric arrangements of the light source and the photo detector. Specifically, in the transmission mode, a tissue sample is placed between the light source and the photo detector, while in the refection mode, the source of light and detector are placed side by side. In the transmission mode, the photo detector has to detect the light transmitted through the tissue, and, thus, the measurement site may be limited to tissues where transmitted light can be readily detected, e.g., fingertips and earlobes.

IPPG INSTRUMENTATION

The key part of an IPPG system is the camera, which collects the reflected or transmitted photons from the skin. The camera's characteristics significantly influence the recorded images and, consequently, the physiological parameters. Making use of the cellphone based IPPG system, the embedded digital camera for image videoing mode and white LED (the flashlight) as the light source positioned at the back of a cellphone serves as our instrument.

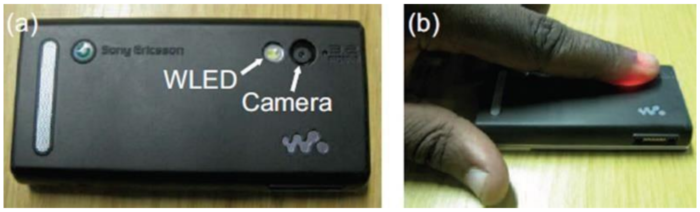


Figure 3.4. A cell phone based IPPG system

The image labelled (a) shows position of the video unit comprising a white LED (WLED) and camera. The image labelled (b) shows light PPG imaging of the index finger positioned to cover the cell phone video unit.

STEPS FOR LOGIN IN

i. Get Username and Password
ii. If user name in database is equal to the entered username and the password is equal to the entered Password. iii. Then login successful.
Iii Else, login failed.

Table 2. Table for Admin

Field	**Data Type**	**Size**	**Attribute**	**Null**	**Default**	**Extra**
Id	Int	11		No	none	AUTO_INCREMENT
Username	Varchar	50		No	none	
Password	Int	4		No	none	
Name	Varchar	100		No	none	

Table 3. Table for User Login

Field	**Data Type**	**Size**	**Attribute**	**Null**	**Default**	**Extra**
Id	Int	11		No	none	AUTO_INCREMENT
Username	Varchar	50		No	none	
Password	Int	4		No	none	
Name	Varchar	100		No	none	

SYSTEM FLOWCHART

A flowchart is a diagram that represents an algorithm, workflow or process, showing the steps as boxes of various kinds, and their order by connecting them with arrows. This diagrammatic representation illustrates a solution model to a given problem. Flowcharts are used in analysing, designing, documenting or managing a process or program in various fields. The system flowchart as shown in Figure 4.9.

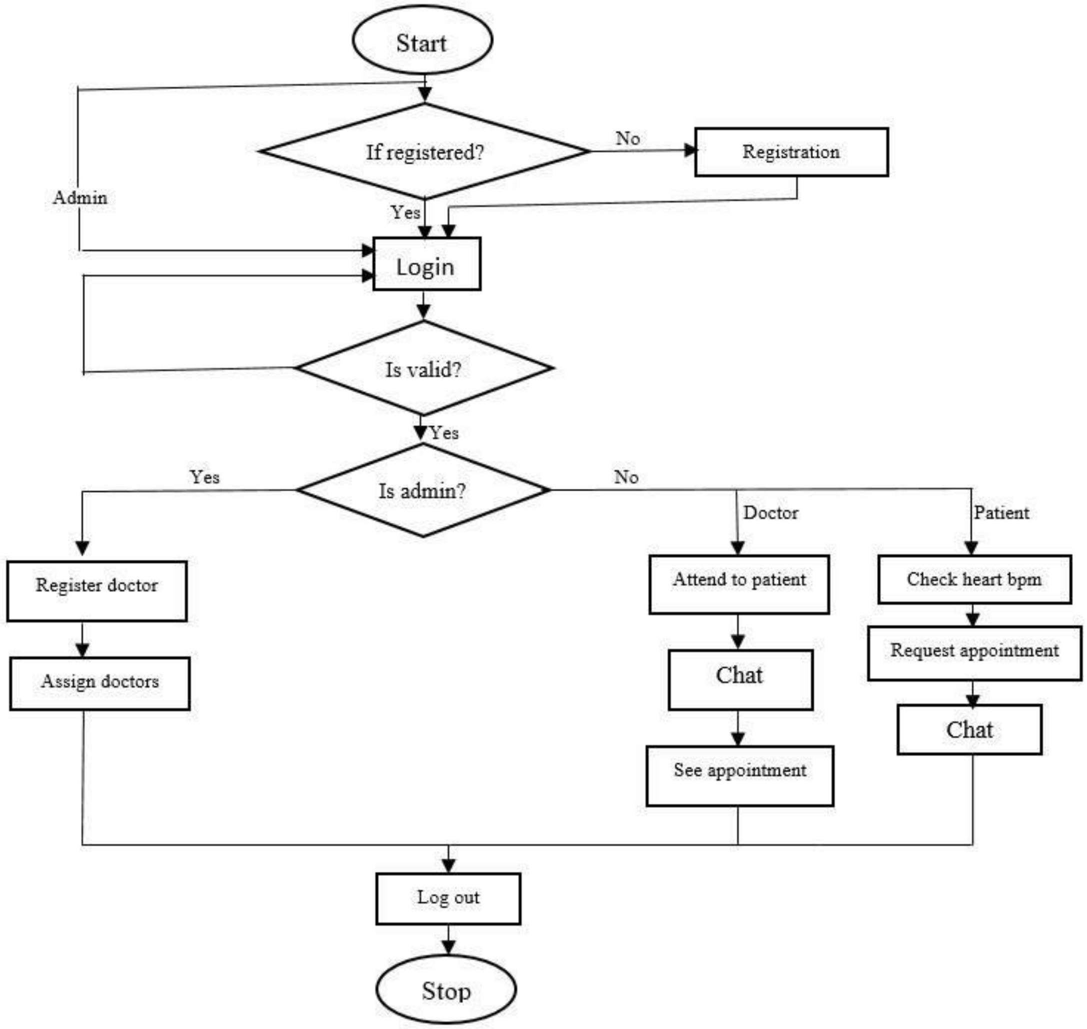
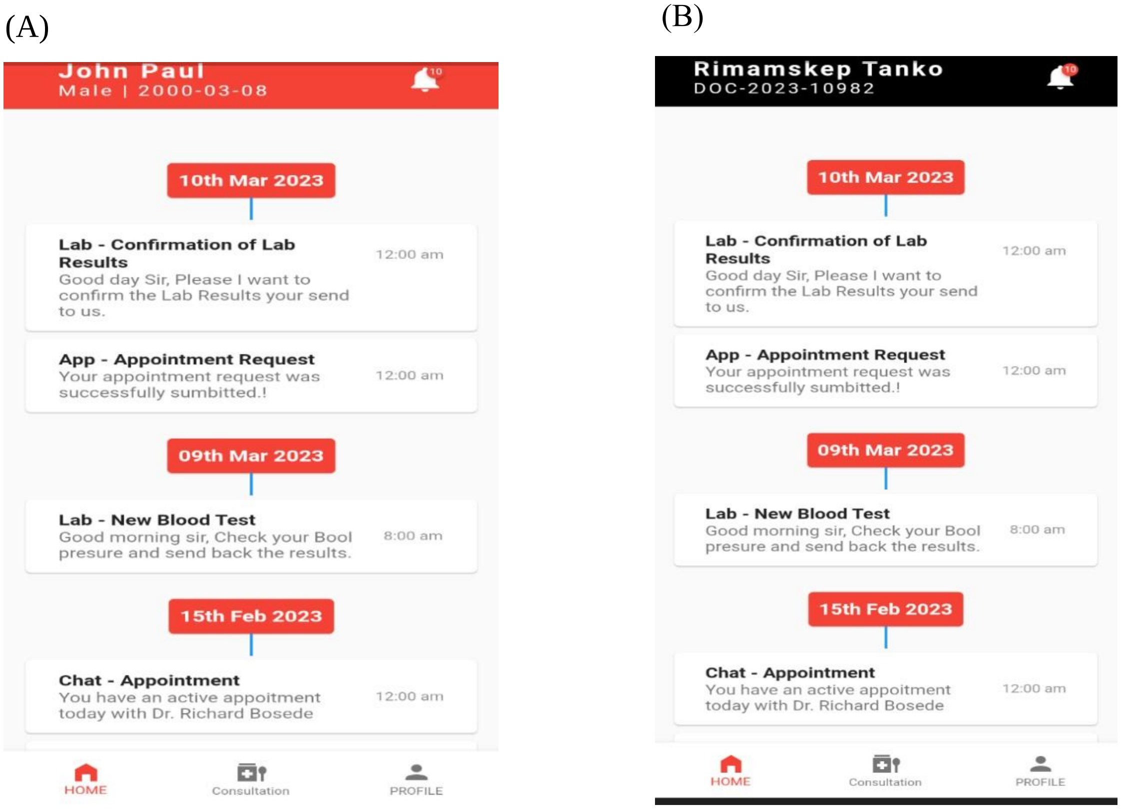


Figure 3.5. System Flowchart

RESULTS AND DISCUSSION

Home Page

This is the first page that pops up when a patient, doctor or administrator logs into their account. The page contains several links to other pages. The figures below shows the home page of the three different users of the system. Figure A shows the home page of a patient, B shows that of a doctor and C of the administrator.



(A)

John Paul
Male | 2000-03-08

10th Mar 2023

Lab - Confirmation of Lab Results 12:00 am
Good day Sir, Please I want to confirm the Lab Results your send to us.

App - Appointment Request 12:00 am
Your appointment request was successfully sumbitted.!

09th Mar 2023

Lab - New Blood Test 8:00 am
Good morning sir, Check your Bool presure and send back the results.

15th Feb 2023

Chat - Appointment 12:00 am
You have an active appoitment today with Dr. Richard Bosede

(B)

Rimamskep Tanko
DOC-2023-10982

10th Mar 2023

Lab - Confirmation of Lab Results 12:00 am
Good day Sir, Please I want to confirm the Lab Results your send to us.

App - Appointment Request 12:00 am
Your appointment request was successfully sumbitted.!

09th Mar 2023

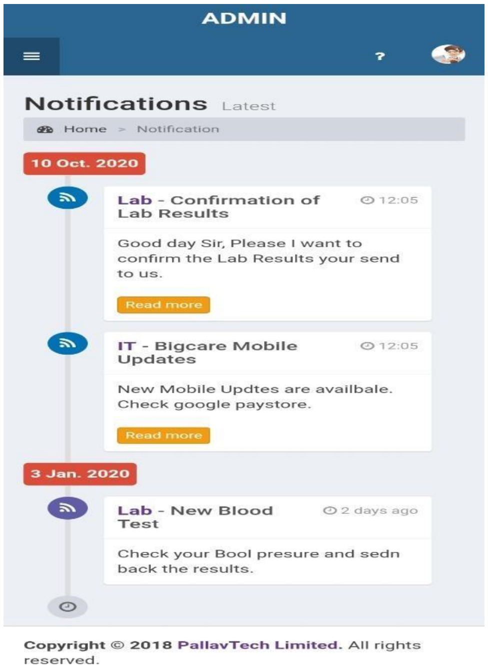
Lab - New Blood Test 8:00 am
Good morning sir, Check your Bool presure and send back the results.

15th Feb 2023

Chat - Appointment 12:00 am
You have an active appoitment today with Dr. Richard Bosede

4.1 system home page

(C)



ADMIN

Notifications Latest

Home > Notification

10 Oct. 2020

Lab - Confirmation of Lab Results 12:05
Good day Sir, Please I want to confirm the Lab Results your send to us.
Read more

IT - Bigcare Mobile Updates 12:05
New Mobile Updtes are availbale. Check google paystore.
Read more

3 Jan. 2020

Lab - New Blood Test 2 days ago
Check your Bool presure and sedn back the results.

Copyright © 2018 PallavTech Limited. All rights reserved.

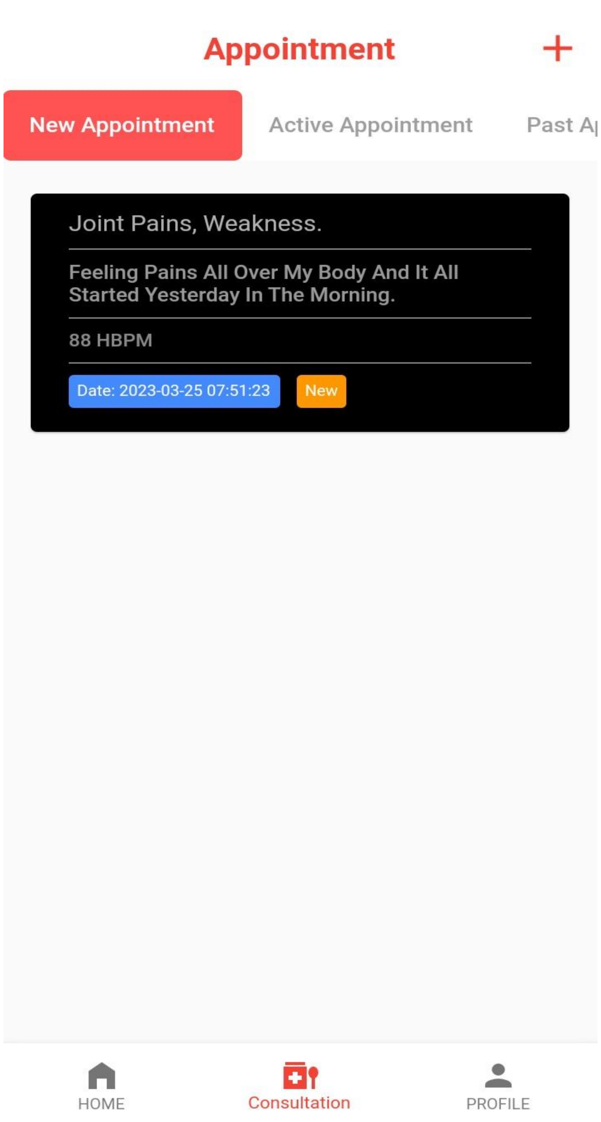
Figure 4.2. System Home Pages

REGISTER PAGE

On this page, a patient registers before getting access to a username and a password. During the registration process, the visitor makes use of a valid email address as a username and chooses a pin.

DOCTOR DASHBOARD

This is the personal dashboard of a doctor where the doctor can know the patient(s) assigned to him/her, chat (communicate) with a patient during the consultation session, view new, active and past appointments and lastly, the doctor can get to view the profile of the patient.



Joint Pains, Weakness.

Feeling Pains All Over My Body And It All Started Yesterday In The Morning.

88 HBPM

Date: 2023-03-25 07:51:23 New

Figure 4.4. Doctor Dashboard

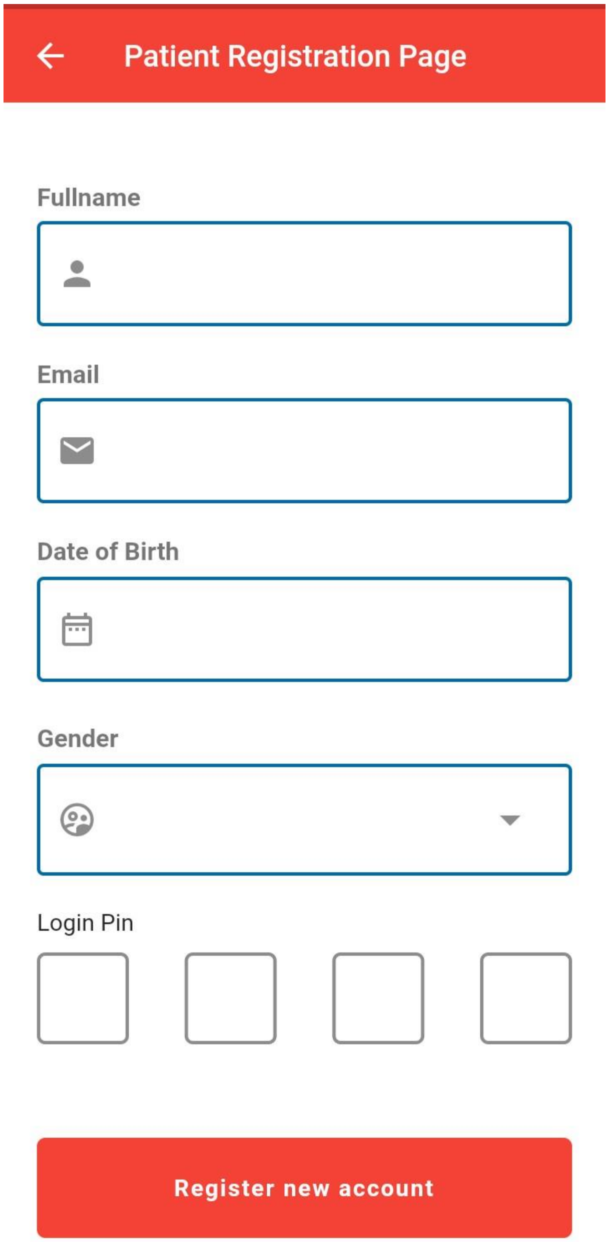


Figure 4.5. Register Page

SUMMARY

This work proposes integrating the Advanced Encryption Standard (AES) algorithm into Internet of Things (IoT) devices used in telemedicine to enhance the security and privacy of sensitive patient data. The approach emphasizes:

Flexible AES Key Lengths: Supporting AES-128, AES-192, and AES-256 to balance security and device performance.

Hardware Acceleration: Utilizing cryptographic hardware modules for efficient encryption on resource-limited medical devices.

Hybrid Security: Combining AES with Elliptic Curve Cryptography (ECC) for secure key exchange and SHA-256 for key integrity.

Real-Time End-to-End Encryption: Encrypting patient biosignals at the device level before transmitting to cloud storage, ensuring data confidentiality during transfer and storage.

Cloud Integration: Safeguarding electronic health records (EHRs) in the cloud, allowing only authenticated clinicians to access decrypted data.

Lightweight Alternatives: Considering ultra-lightweight

RECOMMENDATION FOR FEATURE WORK

The world has since turned in to a global village since the advent of technology. Hybrid Encryption: Combine AES with Elliptic Curve Cryptography (ECC) for key exchange and SHA-256 for key hashing. This reduces key size while maintaining robustness, ideal for multi-user telemedicine platforms. Pairing AES with encrypted cloud storage for EHRs, ensuring only authorized clinicians access data via authentication layers.

CONFLICT OF INTEREST

The authors have no conflict of interest.

REFERENCES

Abdullah, A. M. and Aziz, R. H. H. (2016). New Approaches to Encrypt and Decrypt
Data in Image using Cryptography and Steganography Algorithm. International Journal of Computer Applications. 143, 11-17.

Akhil, K. M., Praveen, K. M. and Pushpa, B. R. (2017). Enhanced Cloud Data Security Using AES Algorithm. 2017 International Conference on Intelligent Computing and Control (I2C2). 2018, 1-5.

Anand, D. and Scholar, R. (2019). A Survey and Learning Techniques on Access Controls in Cloud Computing. International Journal of Research in Advert Technology. 2, 234240.

Andrews, L. J., Baptist, L. R. and Shanmugasundaram, S. (2019). Mobile Andriod-based Remote Patient Monitoring System through Wearable Sensors. Journal of Discrete Mathematical Sciences and Cryptography. 4, 557-568.

Britannica (2021). Diagnosis. Retrieved November 16, 2021, from:
https://www.britannica.com/science/diagnosis.

Cloud Computing Tutorial. Retrieved November 16, 2021, from:
https://tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf

Corinne, B. M. C. (2021). Advanced Encryption Standard. Retrieved March 2, 2023, from:
https://www.google.com/amp/s/www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard%3famp=1

de Cleber, M. M., Sadok, D., and Kelner, J. (2019). An IoT Sensor and Scenario Survey for Data Researchers. Journal of the Brazilian Computer Society. 1, 4.
Ganiga, R., Pai, R. M., Pai, M. M. M. and Sinha, R. K. (2018). Private Cloud Solution for Securing and Managing Patient Data in Rural Healthcare System. 3rd International Conference on Computer Science and Computational Intelligence. 135(2018)688699.
Gogia, S. (2020). Fundamentals of Telemedicine and Telehealth. London, Academic Press. 11.
Hidayat, T. and Mahardiko, R. (2020). A systematic Literature Review Method on AES Algorithm for Data Sharing Encryption on Cloud Computing. International Journal of Artificial Intelligence Research. 4, 49-57.
Islam, N. K. V. and Riyas, M. K. V. (2017). Analysis of Various Encryption Algorithms in Cloud Computing JCSMC. International Journal of Computer Science and Mobile Computing. 6, 90-97.
Jordi, S. and Santiago, S. (2017). Internet of Things. Czech Technical University of Prague Faculty of Electrical Engineering ISBN 978-80-01-06232-6. Retrieved November 16, 2021, from: https://core.ac.uk/download/pdf/132530214.pdf.
Khan, M. F. F. and Sakamura, K. (2012). Context-aware Access Control for Clinical Information Systems [Paper Presentation]. In: Innovations in Information Technology (IIT), International Conference, Abu Dhabi, United Arab Emirates.
Khandpur, R. S. (2017). Telemedicine Technology and Applications: mHealth, TeleHealth and eHealth. PHI Learning Pvt. Ltd. 19-20.
Khelifi, F., Bradai, A., Benslimane, A., Rawat, P. and Atri, M. (2019). A Survey of Localization Systems in IoTs. Mobile Network Application. 24, 761-785.
Kramp, T., Kranenburg, R. V. and Lange, S. (2013). Introduction to the Internet of Things. Business. 6, 1-6. Krishna, V. (2020). IoT Sensor Market. Retrieved September 18, 2021, from: https://communalnews.com/ms/pasaran-sensor-iot/.
Lakshmi, M. D. and Dhas, J. P. M. (2011). An open source private cloud solution for rural healthcare [Paper presentation]. 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, pp. 670–674.
Lee, B. H, Dewi, E. K. and Wajdi, M. F. (2018). Data Security in Cloud Computing Using AES Under HEROKU Cloud [Paper presentation]. The 27th Wireless and Optical Communications Conference (WOCC2018), Hualien, Taiwan.
Medhat, G. M., Aneiba, A., Basurra, S., Batty, O., Elmisery, A. M., Kovalchuk, Y. (2019). IoTs and Data Mining: From Applications to Techniques and Systems. Wiley Interdisciplinary Review Data Mining and Knowledge Discovery. 9, 1292.
Mohammad, W. and Abdellatif, M. M. (2019). Telemedicine: An IoT Application for Health care Systems. Proceedings of the 2019 8th International Conference on Software and Information Engineering (pp. 173-177).
Narendra, S., Abhineet, A. and Akhtar, H. (2020). Cloud Based Healthcare Services for Telemedicine Practices using Internet of Things. Journal of Critical Reviews. 7, 23945125.
Raghavendra, G., Radhika, M. P., Manohara, P. M. M. and Rajesh, K. S. (2018). Private Cloud Solution for Securing and Managing Patient Data in Rural Healthcare System. 3rd International Conference on Computer Science and Computational Intelligence, pp. 689-696.
Rolim, C. O., Koch, F., Westphall, C. B. and Werner, T. (2010). A Cloud Computing Solution for Patient’s Data Collection in Health Care Institutions. Second Internnational Conference on eHealth, Telemedicine, and Social Medicine, pp. 95-99.
Sidorov, V. and Keong, W. Ng. (2015). Transparent Data Encryption for Data-in-Use and Dataat-Rest in a Cloud-based Database-as-a-Service Solution. Conference Paper, pp. 1-5.
Stothart, C., Mitchum, A. and Yehnert, C. (2015). The Intentional Cost of Retrieving a Cell Phone Notification. Journal of Experimental Psychology. 4, 893-897.
Sun, Y. and Thakor, N. (2015). Protoplethysmorgraphy revisited: from contact to noncontact, from point to imaging. IEEE Transactions on Biomedical Engineering. 63(3): 463477.
Tom, L. and Prakash, N. (2012). Cloud Computing Deployment Models. Retrieved November 26, 2021,from: https://www.sciencedirect.com/topics/computerscience/clouddeployment-model.
Tutorialspoint (2021). Cloud Computing Tutorial. Retrieved November 16, 2021, from: https://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf.