I.J. Information Technology and Computer Science, **2023, 1, 9-20**
Published Online on February 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2023.01.02

A Trust Management System for the Nigerian Cyber-health Community

Ifeoluwani Jenyo
Computer Sciences Department, Adeleke University, Ede, Nigeria
E-mail: jenyoifeoluwani@gmail.com
ORCID iD: https://orcid.org/0000-0003-1125-2249

Elizabeth A. Amusan*
Cyber Security Science Department, Ladoke Akintola University of Technology, Ogbomoso.
E-mail: eaadewusi@lautech.edu.ng
ORCID iD: https://orcid.org/0000-0003-4134-5497
*Corresponding author

Justice O. Emuoyibofarhe
Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso.
E-mail: eojustice@gmail.com
ORCID iD: https://orcid.org/0000-0003-1211-5182

Received: 05 July 2022; Revised: 21 September 2022; Accepted: 03 November 2022; Published: 08 February 2023

Abstract: Trust is a basic requirement for the acceptance and adoption of new services related to health care, and therefore, vital in ensuring that the integrity of shared patient information among multi-care providers is preserved and that no one has tampered with it. The cyber-health community in Nigeria is in its infant stage with health care systems and services being mostly fragmented, disjointed, and heterogeneous with strong local autonomy and distributed among several healthcare givers platforms. There is the need for a trust management structure for guaranteed privacy and confidentiality to mitigate vulnerabilities to privacy thefts. In this paper, we developed an efficient Trust Management System that hybridized Real-Time Integrity Check (RTIC) and Dynamic Trust Negotiation (DTN) premised on the Confidentiality, Integrity, and Availability (CIA) model of information security. This was achieved through the design and implementation of an indigenous and generic architectural framework and model for a secured Trust Management System with the use of the advanced encryption standard (AES-256) algorithm for securing health records during transmission. The developed system achieved Reliabity score, Accuracy and Availability of 0.97, 91.30% and 96.52% respectively.

Index Terms: Cyber-health, Nigeria, Privacy, Reputation, Security, Trust Management.

1. Introduction

Cyber Health is defined as "a condition of cyber systems and networks that are not only free from malware and botnets infection but also contributes more broadly to the overall trust and usability of the cyberspace for the well-being of all" [1]. In Nigeria, health care systems and services are mostly fragmented, disjointed, heterogeneous with strong local autonomy and distributed among several healthcare givers platforms which may be public or private [2,3]. The Cyber-health and its community in Nigeria is still in its infant stage with more participants (healthcare workers, administrators, ICT workers and other stakeholders) joining every day. This makes it pertinent for the community to interact, explore and share resources which is only possible if there is trust among them. Trust is considered an indicator of quality of care and is associated with patients' satisfaction [4].

The awareness, adoption and acceptance rate is low with few healthcare centers having electronic health records. Even those that have e-records did not secure it, thereby making privacy breaches a concern. Healthcare centers are reluctant in releasing the e-records of their patients to other centers for fear of theft, misuse and loss of internal revenue. While healthcare technologies play key roles in our populations' health, they are vulnerable to security threats due to interconnections, easily accessible access points, outdated systems and lack of emphasis on cyber security [5-7]. Although Information and Communication Technology (ICT) in health holds great promise to significantly improve the quality and delivery of healthcare service, the security, privacy and confidentiality of patients' records across computer networks

remain a serious concern.

Delivering e-health services across multiple cloud providers requires a trustworthy brokering framework [8]. Such framework should be capable of ensuring that the integrity of shared patient information among multi-care providers is preserved and that no one has tampered with it. Trust in e-Health is the quantified belief by a trustor with respect to the honesty, competence, security and dependability of a trustee within a specified context [9]. Although, several approaches (cryptographic and non-cryptographic) exist in literature for ensuring security and privacy of e-health data [10-12], the quest for an optimal solution remains unanswered.

A leading approach to trust management is Reputation. Reputation is based on trust and on past behavioral record of an entity. However, reputation-based systems are limited in managing first time threats to the system because every criminal has a first time. Another method of ensuring trust is through performing Real-Time Integrity Check (RTIC) which involves an online or real-time check to ascertain the integrity of any requesting entity for access. This is a real-time assessment of the reputation of the entity over the internet before requesting for access. This is based on the Confidentiality, Integrity, and Availability (CIA) model which are considered the three most crucial components of security. The Real-Time Integrity Check evaluates which criteria to know if any of the three elements has been compromised in the requesting entity.

This study is aimed at developing a Trust Management System for guaranteed privacy and confidentiality within the networked community of patients, healthcare providers and health records across hospitals. Hence, the objectives are to first, design a model and architectural framework of the trust management system. The second objective is to implement the designed model and lastly, evaluate the performance of the developed system using both objective and subjective evaluation techniques. Therefore, the paper presents a framework that will go a long way to put the Nigeria cyber-health network in proper perspective and mitigate vulnerabilities to privacy thefts. This paper is organized as follows: Section 2 discusses related works. Model design and framework architecting which constitute the Methodology are discussed in Section 3. The result, which is the developed system is presented in Section 4. Section 5 discusses the performance evaluation while the final section presents the conclusion and future work to be done.

2. Related Works

Agent-To-Agent Reputation-Based Trust Management framework for a CACIP based mobile environment was developed by [13]. The work proposed an agent-based trust management model in which, components do not interact directly to share services however, each component that wants to provide service attaches the message/service in the information bus to make it available for other components.

Reference [14] developed a dynamic trust negotiation framework for flexible e-health collaboration within a circle of trust (COT). The authors proposed a decentralized approach to trust negotiation, whereby, entities in a network delegate their trust negotiation task to a third-party entity they both trust. Once this trusted party can establish trust between with the entity requesting and with the entity granting access, they do not need to interact directly, access is granted. However, this solution is only feasible for networked parties such as research, academia and public institutions. It is not practical for an open internet era where requests can be made from any requesting entity not previously defined and who do not have existing trust contracts.

Tormo et al, 2013 in their work, Identity Management in Privacy We Trust: Bridging the Trust Proposed a distributed reputation model to determine a specific entity's trustworthiness while preserving users' and entities' privacy. Model aggregates recommendations, it doesn't know users' or other entities' recommendation values about a specific entity. It also keeps secret the reliance that a specific entity gives to its recommenders, used to compute reputation values. However, there is still the inability to ensure the privacy of reputation feedback provider as reputation is a reliance on past behavior, hence, its limitation.

HealthyBroker: A Trustworthy Blockchain-based Multi-Cloud Broker for Patient-Centered eHealth Services was presented by [8]. They opined that one technology that can help brokering systems achieve trust is the block chain technology which can be used to build trust-worthy ecosystems for distributed environments. However, this requires distributed ledger, that is, block chain which has not gained widespread adoption as it is still reliant on reputation which is historic behavior.

Arising from the reviewed works in this section, it is evident that trust is an underlying phenomenon of any security system and the demand for an optimal solution remains unanswered as existing models fall short in addressing this special requirement of patient-centered ehealth services holistically. Our approach therefore proposes a way forward by designing a trust management framework in response to the need of the expanding cyber-health community in Nigeria, and by extension, other developing nations of the world.

3. Research Methodology

Towards achieving the set objectives of this research, it adopted a design and experimental approach for the development of the trust management system. Thus, a framework and model was designed with underlying assumptions for the trust management system. The framework was built using the 3-tier client-server architecture which consists of the client tier, application server tier and the web server tier. The designed model was implemented using the Laravel

framework which is a PHP-based web implementation framework. The client tier of the system was implemented as web services while the server tier was implemented using the WAMP (Windows, Apache, MySQL and PHP) server. The last objective was achieved by carrying out a performance evaluation of the developed system using both objective and subjective evaluations.

3.1. Framework Development Assumptions

The Trust Management Architectural framework developed in this work was premised on the following underlying assumptions:

- There exists a network of hospitals and ICT infrastructures as depicted in Fig 1.
- The Healthcare Information is hosted on a centralized online database, not kept independently by any entity or moved around within the system.
- A requesting entity on authorization can only access the EMR to read and/or update it.
- The requesting Entity can be the Patient.
- The requesting Entity can be the Doctor, Pharmacist or any other healthcare service Stakeholder, however, patient authorization is required.
- Any Entity makes the request over a digital infrastructure; network (e.g. the internet) phone, tablet, PC, and many more.

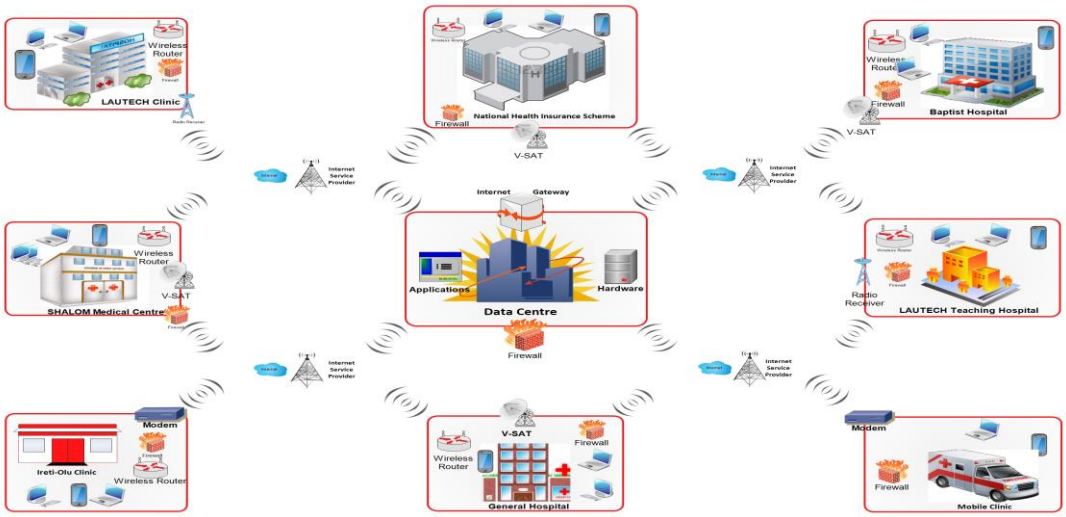

Fig.1. An Evolving Distributed-Centralized Health Infrastructure Model of Selected Hospitals in Ogbomoso [15].

3.2. The Hybridized Trust Management Model

The Real-Time Integrity Check (RTIC) was combined with the reputation based approach to get the best of both worlds, such that every requesting entity is at first taken through a Reputation Test. Only entities that pass the reputation test are taken through the Real-Time Integrity Check. A margin of failure will be given such that if the requesting entity does not cross a threshold of bad reputation, it cannot go through the Real-Time Integrity Check.

Every result of the Real-Time Integrity Check also becomes an input for the Reputation Database used for the Reputation Assessment as shown in Figures 2 and 3 respectively, the hybridized model was used to develop the Trust Management Framework shown in Fig. 4.

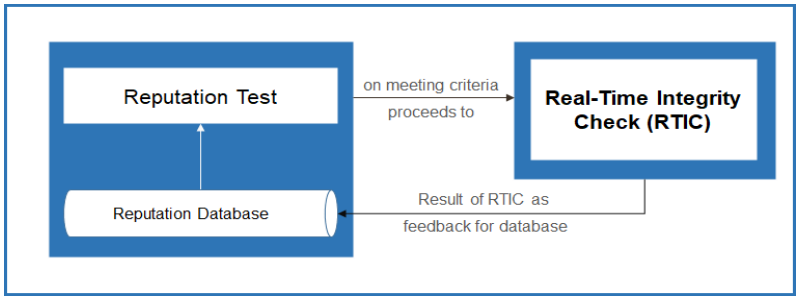

Fig.2. Combining the Two Complementary Approaches.

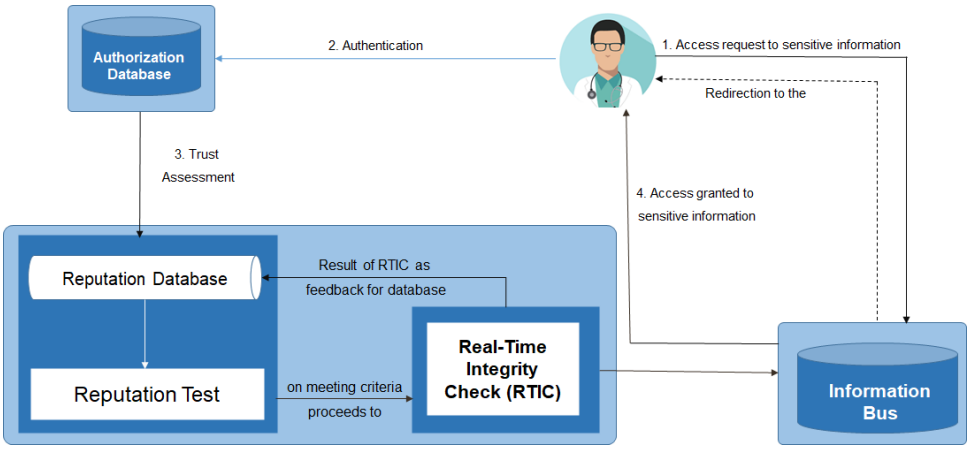

Fig.3. Components of the Trust Management Model.

Hence, Fig. 4 is the proposed Trust Management Framework for Guaranteed Privacy and Confidentiality for the Nigerian Cyber-health Community and it is made up of three distinct layers which are the presentation (user interface), broker (application) and resource (infrastructure) layers respectively.

The presentation layer is concerned with managing all user interaction and presenting information to the user. This is where all graphical user interface (GUI) for the various levels of inputs, data capturing and communication with the system is presented. This layer houses the login form for patient and doctors, appointment scheduling interface, patient-doctor consultation interface, transfer authorization interface, encryption/decryption interface and report generation/viewing forms.

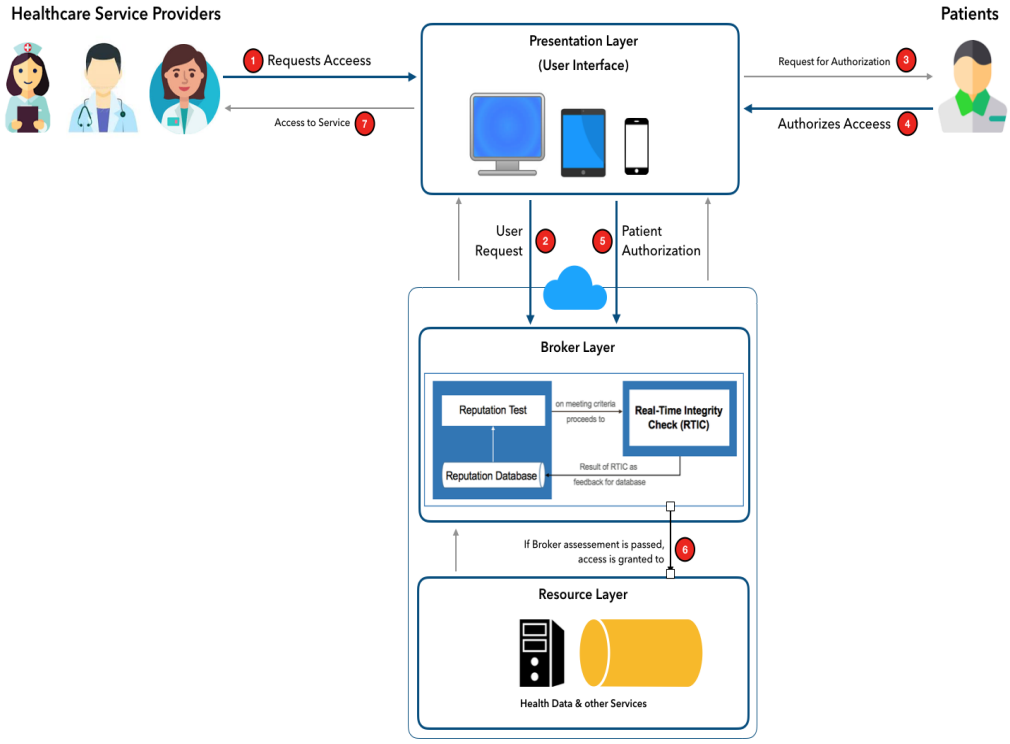

Fig.4. Trust Management Framework for Guaranteed Privacy and Confidentiality.

The broker layer which is also the application layer is concerned with implementing the logic of the application and so providing the required functionality to end users. It also handles all security related activities such as: authentication and authorization, verification, data integrity, encryption/decryption.

The resource layer which is the third stores data and provides transaction management services and further manages the data that is passed to and from the client. This layer consist of several databases for storing and handling communication logs, data control, data integrity checks, reputation database etc.

3.3. Framework Architecting

To further describe how the components of the proposed framework are functionally and logically related, the

framework's architecture was done adopting the 3-tier client-server architecture because it is a distributed architecture and is typically used when there are different categories of transactions to be processed differently by divers servers' logics. The 3-tier architectural solution as shown in Fig. 5 is comprised of the client tier, application server tier and the web server tier as described here in this subsection.

A. Client Tier

The Client tier consists of the Doctor's computer, Patient computer or mobile device, and web browser. The mobile device uses Wireless Application Protocol (WAP) to connect through the web browser to obtain web services. The client layer provides interfaces that allows a user (doctors' computer or patients' mobile terminal) interact with the program running on the server through a web browser or phone-based application. The browser is responsible for presenting the markup from the application server as web forms.

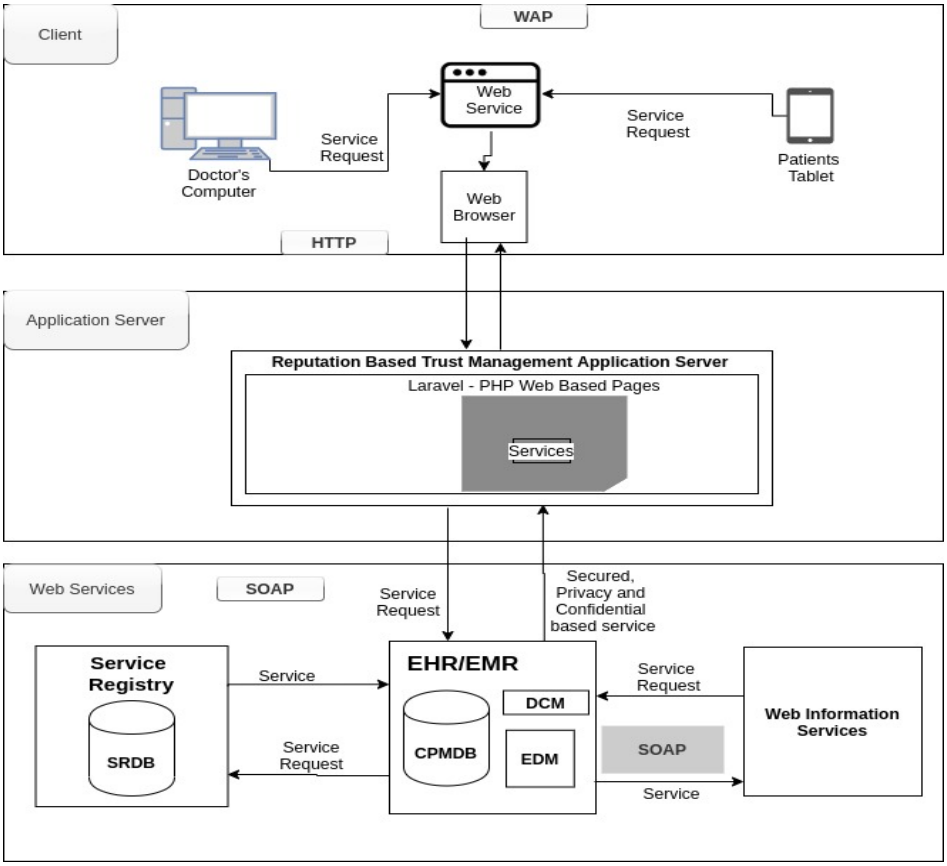

Fig.5. The Designed Trust Management 3-Tier Architecture.

B. The Application Server Tier

The Application Server layer consist mainly of the reputation based trust management system built using the Laravel PHP Web Server framework. The application server is responsible for executing requests from the client side to the Context Profile Manager (CPM). It is also responsible for implementing application-specific logic as well as information storage and retrieval requests; which include the following:

- Registers new patients and doctors, and forwards their profiles to the Context Profile Manager Database (CPMDB).
- Provide Authentication and authorization
- Provides encryption and decryption services on patient health records, computes and generates appropriate reputation index for doctors
- Content management

C. The Web Server Tier

The web server layer consists of the CPMDB, and Service Registry. The CPMDB is responsible for managing patient and doctor's profile and dynamic content manager (DCM) while Service Registry is responsible for services' registration. The web server is responsible for all user communications, with the user interface implemented using a web browser. This is made possible using service-oriented architecture (SOA), and particularly, the simple object access protocol (SOAP).

3.4. System Design, Implementation and Tools

The model driven development (MDD) approach was adopted in this research. It is an approach to software engineering centered on system models that are expressed in the unified modelling language (UML). A system flowchart (SFC) that shows the system flow stage wise and in a logical sequence is depicted by Fig. 6. The earlier presented architectures and designed models were used to implement the trust management system for simulation of the developed framework as a client-server system using Laravel framework. Laravel is a PHP-based web framework whose choice was informed because it is very expressive, well designed with simple and fast routing engine as an implementation framework. In addition to PHP programming language, other tools used for the implementation of this work are HTML, CSS, Bootstrap and WAMP Server.

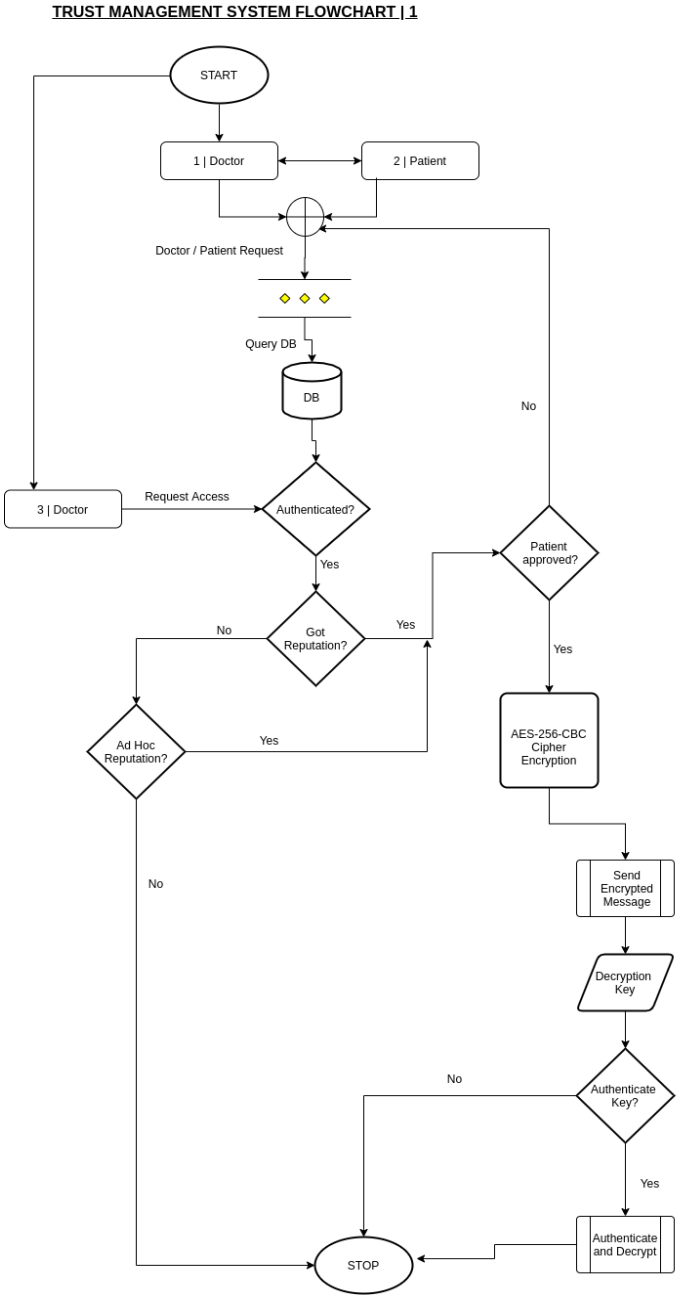

Fig.6. The Trust Management System Flowchart.

The client side of the trust management system was implemented essentially as web services view and web pages using PHP7, HTML5 and CSS3 while the server side implementation of the trust management system was achieved using the server side code of PHP running on WAMP server version 5.0 (WAMP5).

3.5. Encryption and Decryption Algorithm Used

As part of the functional requirements of the proposed framework to ensure security and provide privacy and

confidentiality of patient health records handling and during transfer, information hiding was achieved using the popular Advanced Encryption Standard (AES-256) algorithm as shown in Fig. 7. The choice of the encryption algorithm was informed based on the fact that it is widely regarded as the most secure symmetric key encryption cipher.

AES-256 ENCRYPTION/DECRYPTION ALGORITHM

Step 1:	Start
Step 2:	Authenticate Doctor's session id
Step 3:	Set Encryption Key
Step 4:	Derive the set of round keys from the cipher key
Step 5:	Initialize the start array with the medical report (plaintext)
Step 6:	Add the initial round key to the starting state array
Step 7:	Perform nine rounds of state manipulation
Step 8:	Copy the final state array out as the encrypted data (ciphertext)
Step 9:	Sign encrypted data with a message authentication code (MAC)
Step 10:	Store encrypted data in the DB
Step 11:	Stop

Fig.7. AES-256 Encryption Algorithm.

Furthermore, access to a service is granted to the requesting entity if conditions are met.
The Reputation Index calculated in percentage is:

$$R_V = D_{ri} + D_{nr} + (G_A - B_A) / T_A * 100 \quad (1)$$

If $D_{nr} <= 20$ then

- R_V: a reputation value for each agent that determines it's trustworthiness.
- G_A: number of good actions an agent has done when it was accessing resources.
- B_A: number of bad actions an agent has done when it was accessing resources.
- T_A: total number of actions an agent has done.
- P_V: a reputation value from Patients authorization.

4. Results and Discussion

The developed trust management application was installed on both a stand alone system and networked systems to enable adequate testing of the client side, the server side of the system and the various network communications. In this section the outputs of the client side of the system will be presented as this consist majorly of the user interfaces that the doctors, hospital staff and patients use to interact with the system, other outputs of the client side of the system include web forms and report forms. The outputs of the server side of the system are not visibly seen but their performance in terms of the some of the functional requirements were presented in the evaluation of the system overall performance.

On launching the application, the home page dashboard is first displayed and the login page is presented for login either as a staff, doctor or patient as in Fig. 8. This is so because the system adopts the role-based access mechanism to assign responsibilities to the users who can either be a Patient, Medical Expert or Administrator. Only patients with existing record in the hospital can login to either schedule an appointment or have a consultation session with the doctor and posiibly view their health record. New patient must have their new files created by the administrator during their first visit at the hospital. Doctors already registered in the system can edit patient health record, append case notes and athourized referral or authorize patient to give consent for file transfer etc. To login into the account, the user is required to submit user's email address and users' login id.

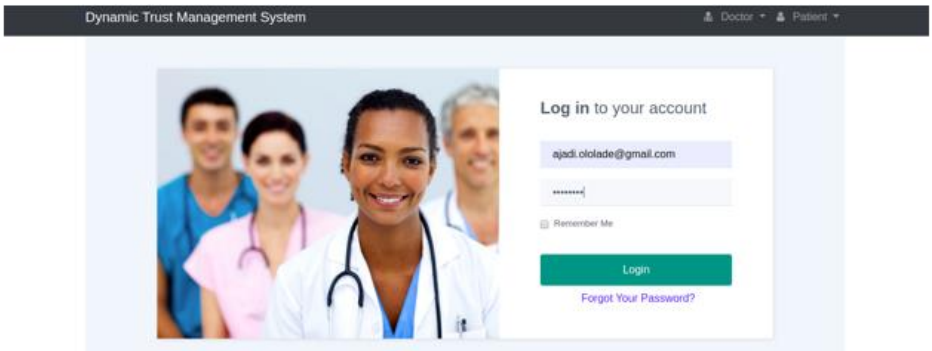

Fig.8. The Login Interface.

Fig. 9 shows a general report dashboard identifying the doctor that logged in as Dr. Paul Ajadi. The list of possible activities the doctor have access to are listed to the left of the screen which include access to patient, view medical records, transfer files. The report dashboard also shows highlighted pictorial views of other forms of results the system provides. For example, it indicates that a total of 180 doctors are currently registered and available on the entire system, with different areas of specialization and level of expertise. While doctors have access to most other doctors, patient do not have access to all doctors. The figure also shows that a total of 200 patients are registered on the system with a total of 15 laboratories, the rating of doctors based on their reputation and trust index can also be viewed. Three (3) recently encrypted reports decrypted and viewed by a doctor whose name appears on the report are also indicated in the Figure.

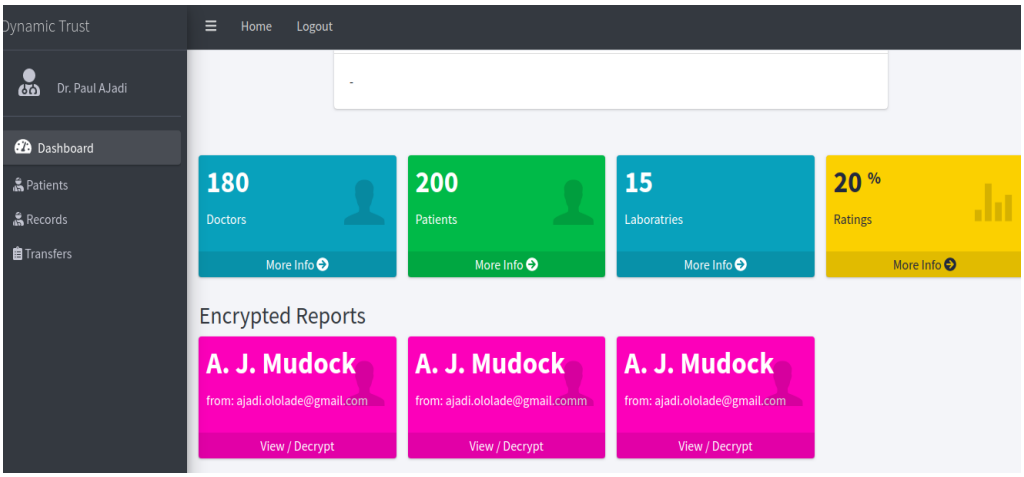

Fig.9. General Report Dashboard View.

One of the main goals of this work is to provide secure communication among care givers that guarantee privacy and confidentiality during transmission of patient health records. This was achieved by making sure that every patient file transferred to any other section or department or from one doctor to another doctor is encrypted using AES 256 encryption algorithm and the decryption keys sent via email to only the expected recipient, and vice versa. Fig. 10 shows the doctor-to-doctor communication interface with data encryption and decryption features.

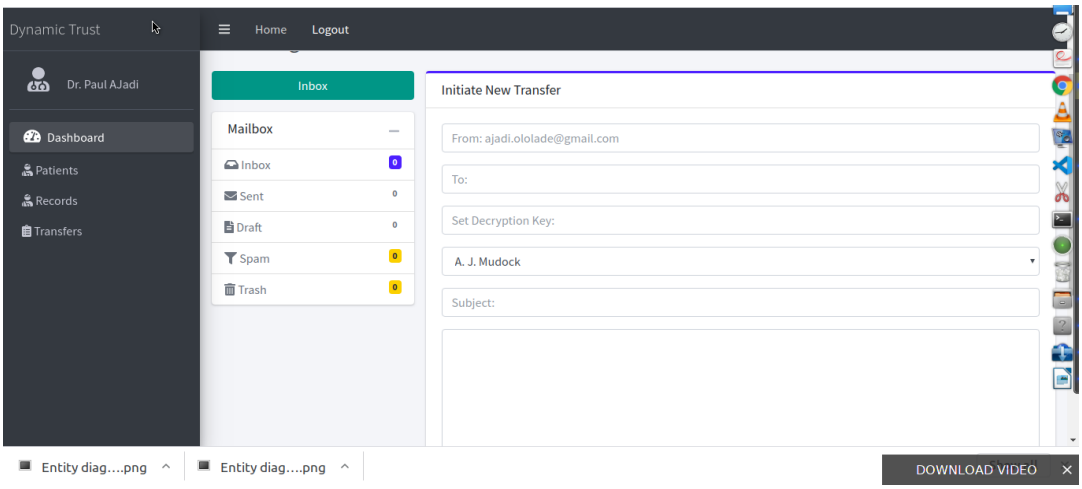

Fig.10. The Encryption Interface.

5. Performance Evaluation

The efficiency of the developed prototype was evaluated in two phases. First, objective evaluation was carried out in terms of reliability and availability. The second was subjective evaluation which was user-centered in terms of system ease of usage and degree of relevance.

Objective Evaluation

Table 1 shows the data obtained from the system during six (6) different testing experiments of 10 hours per day for 6 days. The data obtained were used to evaluate the system performance based on reliability and availability. The efficiency of the encryption module was also determined. The metrics used for computing reliability of the system were the: uptime, downtime, number of encrypted files transferred, number of received files decrypted, number of failures and

mean time before failure (MTBF).

Table 1. Reliability and Availability Evaluation Analysis Data.

	Test Period (hrs)	Uptime (mins)	Downtime (mins)	No of Encrypted files Sent	No of Decrypted files Recieved	No of Failed Transfer	MTTR (mins)	MTBF (mins)
Exp 1	10	596	4	42	40	2	4	580
Exp 2	10	587	13	55	50	5	13	572
Exp 3	10	597	3	36	36	0	3	588
Exp 4	10	535	65	25	18	7	65	485
Exp 5	10	600	0	30	28	2	0	600
Exp 6	10	560	40	19	17	2	40	530
Total	600	3475	125	207	189	19	122	3355

$$\text{Reliability } R = 1 - \lambda_T \tag{2}$$

$$R = 1 - \frac{19}{600}$$
$$= 1 - 0.03 = 0.97$$

From computation, the system achieved a reliability score of 0.97.

The developed trust-management system was also evaluated for availability. The following metrics were used to represent the availability of the system: expected working time, uptime, response failure, mean time before failure (MTBF), mean time to recover (MTTR).

To compute for system availability A_T,

$$A_T = \frac{Uptime}{\text{Uptime} + \text{Downtime}} \times 100\% \tag{3}$$
$$= \frac{3475}{3475+125} \times 100\%$$
$$= \frac{3475}{3600} \times 100\%$$
$$= 96.52\%$$

The overall system availability is 96.52%, this implies of every ten (10) hours the system was available, up and running for 9.6 hours. The 3.48% of downtime experienced was due to power outage and intermittent network connectivity failure.

Percentage Accuracy of encrypted file transferred.

$$PA_T = \frac{\text{No.of files recieved \& decrypted}}{\text{Total No.of Encrypted files Transfered}} \times 100\% \tag{4}$$
$$= \frac{189}{207} \times 100\%$$
$$= 91.30\%$$

No of files received and decrypted.

Subjective Validation (System Usability Assessment)

A system usability assessment was conducted through the use of questionnaires to assess users experience of the system in terms of ease of use or user friendliness, awareness and involvement of use of HIS, reliability, and level of relevance among others.

The Trust Management System was made available for use by medical practitioners, administrators and ICT experts, after which the questionnaire designed for this research was administered to the users to help analyze the users' experience in terms of the application development tool, users' appreciation of the application, the efficiency and reliability of the system and how secure the system is in relation to trust and reputation.

The questionnaire was administered manually and also automated in the form of a Google form (Https://forms.gle/GigyhyXnvTnX52w8) and circulated online. Out of a total of thirty (30) respondents that filled and returned completely filled questionnaires, twelve (12) are Medical Doctors which represent 40%, three (3) are administrators which represent 10%, and fifteen (15) computer science experts and programmers which represent 50%, respectively. From the spread of the respondents, it can be observed that the medical doctor and hospital administrative staff make up 50% representing a good percentage of end user of the application, of the 50%, 40% are medical doctors, with 10% support staff. On the other hand, 50% of the respondents are core computer programmers with different specializations to ascertain the efficiency and technical quality of the system. The questionnaire consists of a total of 33

questions in five categories, 11 questions are categorical questions of "Yes" or "No" type response while the other 21 questions the questionnaire was developed on a 5-point Likert rating scale, respondents specify their level of agreement to a question or statement. Data was collected using the scale 5 to represent "strongly agree" and 1 to represent "strongly disagree".

Analysis of Response

The respondents' data were analyzed for three categories of effects namely the users' assessment on their perceptions for the system's (i) usability and user friendliness, (ii) relevance of the system and (iii) security and confidentiality or privacy.

Table 2 shows the distribution of the respondents based on the usefulness of the developed system and it will guarantee security and privacy. Out of the thirty (30) respondents, twenty four (24) which represent 80% agreed that the system is useful and it will guarantee security and privacy of patient record while the other 6 respondents (20%) were not in agreement or not certain. This outcome shows that the system is useful in trust management and can guarantee trust, privacy and confidentiality across doctors and patients in various hospitals.

Table 2. Distribution of Respondents Based on Usefulness of Trust Management Application and Whether it can Guarantee Trust, Privacy and Confidentiality across Doctors and Patients in Various Hospitals.

Response	Frequency	Percentage
Useful	24	80.0
Not useful	6	20.0
Total	**30**	**100.0**

Table 3 shows the distribution of the respondents by the performance of the Trust Management System, there are five questions in this category measuring the performance and efficiency of the system and the technology on which the system is built. As can be seen from Table 4.10 the weighted mean score (WMS) for all the questions have values above 2.5. Again, this is an indication overall satisfaction of the performance of the system. Almost all respondents agreed that the system is Web Services based and this had the highest rank. In terms of Patient's Health Record retrieval and Transmission the users found the system to be easy and fast, this question had a 4.24 WMS with the 3rd highest rank. The performance of the system was also evaluated on a peer-to-peer system and a network based client-server environment, the WMS of the respondents were 3.88 and 4.24 respectively. In the overall the respondents agreed that the system performed well, has fast response time and is built on web based technology.

Table 3. The Distribution of the Respondents by the performance of the Trust Management System.

Performance	Weighted mean score	Rank
Patient's Health Record retrieval and Transmission is easy and fast	4.24	3rd
It is Web-Services Based	4.41	1st
Decryption key is always sent to recipient	3.94	11th
It works on peer-to-peer network	3.88	14th
It's a multi-tier Client-Server System and Network based	4.24	3rd

Table 4 shows the distribution of the respondents concerning security, privacy and confidentiality for patient record provided by the system, this category consist of seven questions related to security, privacy and confidentiality. It can be seen from the table that weighted mean score of all the seven questions in this category was more than 2.5 with good ranking. "The system is secure with high level of confidentiality" had a WMS of 4.18 and was ranked 4th.

The system was domain secured with WMS of 3.94 with a very good domain level authorization and authentication credential request of WMS of 4.18 from both doctors and patients, this also ranked 4th. With this application the Patient Privacy is guaranteed had a WMS of 4.19 and ranked 6th. It can be seen that of the seven questions in this category, four major question representing security, privacy and confidentiality out of the seven questions ranked very high, this is an indication from the users experience that the system provides good security, privacy and confidentiality.

Table 4. The Distribution of the Respondents by Providing Security, privacy and Confidentiality for Patient Record.

Security, Privacy And Confidentiality	Weighted mean score	Rank
The system is secure with high level of confidentiality	4.18	4th
Patient's Health Record are secured	3.59	17th
With this application the Patient Privacy is guaranteed	4.19	6th
It guarantees secure EHR transfer	4.06	9th
Requires Doctors authentication and authorization	4.18	4th
Requires patient authentication and authorization	4.18	4th
It is Domain-based secured	3.94	11th

The survey also investigated challenges and barriers that have hindered the adoption and use of ICT, HIS and other related technologies in the hospital which might also hinder the adoption and use of this Trust Management System. The findings are shown in Table 5. 26 out of the 30 respondents representing 86.7% agreed that lack of ICT infrastructure was a major barrier. 20 out of 30 respondents agreed that 66.7% of health worker are ICT Illiterates or have not used ICT in the hospital related services. 80% of challenges encountered on the use of ICT in health is Lack of government policy and standard. However, 18 out of the 30 respondents expressed growing fears by health workers of being replaced by an application or system and hence the slow or lack of interest in ICT or use of HIS.

Table 5. Distribution of the Respondents to the Challenges of use and Adoption of this System in Health Care Delivery.

Challenge	Frequency	Percentage
Lack of ICT	26	86.7
ICT Illiteracy	20	66.7
Unstable power supply	27	90.0
Cultural Belief	15	50.0
Government Policy	24	80.0
Fear by health workers of been replaced by an application or system	18	60.0

6. Conclusion and Future Scope

In this work, we have demonstrated the practicability of developing an indigenous trust management framework for adoption in the Nigeria cyber-health community. The conceptual framework was characterized by a rich blend of Real-Time Integrity Check (RTIC) and Dynamic Trust Negotiation (DTN). With this approach, a reliable method of managing trust is being suggested to facilitate and strengthen collaborations among the various members of the cyber-health community. This framework was explored and implemented within the mobile e-services research group at Ladoke Akintola University of Technology, Ogbomoso, Nigeria which resulted in the prototype of a Trust Management System capable of simulating patients' EHR transfer from doctor-to-doctor or hospital-to-hospital. Also, performance evaluation based on both system-specific metrics and users' assessment of perceived usefulness and relevance was conducted which indicated that the developed system was efficient and useful. In view of the derivable benefits inherent in the use of ICT in the health sector and the vital role of reliable, secure, and confidential patient file transfer, it is recommended that this framework be adopted by both governmental and non-governmental health organizations in Nigeria as a major step towards digital health.

References

[1] Ito Y. (2014): Cyber Green: Improving Cyber Health through Measurement and Mitigation. Japan Computer Emergency Response Team (JPCERT). Available at: https://www.jpcert.or.jp/research/GreenPresentation-20141117_en.pdf.

[2] Clark, T. (2007). Adopting Healthcare Informatics and Technologies. American Journal of Health System Pharmacy, 64.

[3] Stella, O. and Herselman M. E. (2008). E-health in Rural Areas: case of Developing countries. International Journal of Biological and life sciences. 4(4).

[4] Jabeen F., Hamid Z., Akhunzada A., Abdul W. and Ghouzali S. (2018): "Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues," in IEEE Access, vol. 6, pp. 17246-17263, 2018, doi: 10.1109/ACCESS.2018.2810337.

[5] Coventry L. and Branley D. (2018): Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, pp. 48-52. Available at: https://doi.org/10.1016/j.maturitas.2018.04.008

[6] Jalali M.S. and Kaiser J.P. (2018): Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research, 20(5): e10059. Available online at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/.

[7] Iwaya, Ahmad and Babar (2020): Security and Privacy for mHealth and uHealth Systems: a Systematic Mapping Study. IEEE Access.

[8] Kurdi, H., Alsalamah, S., Alatawi, A., Alfaraj, S., Altoaimy, L., & Ahmed, S. H. (2019): HealthyBroker: A Trustworthy Blockchain-Based Multi-Cloud Broker for Patient-Centered eHealth Services. Electronics, 8(6), 602. doi:10.3390/electronics8060602

[9] Grandison, T., (2003): Trust management for Internet Applications, Ph.D. Dissertation, University of London, England, Available at http://pubs.doc.ic.ac.uk/trustmanagem-for-internet-app/trust-managem-forinternet-app.pdf

[10] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019): "eHealth Cloud Security Challenges: A Survey," Journal of Healthcare Engineering, 2019, 1– 15. doi:10.1155/2019/7516035.

[11] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019): "Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing," IEEE Access, 1–1. doi:10.1109/access.2019.2919982

[12] Supriya M. and Rajarajeswari P. (2021): An Efficient Privacy Preserving Approach for e-Health. International Journal of Advanced Computer Science and Applications (IJACSA), 12(4): 157-162.

[13] Nkosi, M., T, Adigun M. O and Emuoyibofarhe, O. J. (2007). IADIS International Conference Applied Computing Texas, ISBN: 978-972-8924(30) 143-150.

[14] Ajayi, R.O., Sinnott, R. and Stell, A. (2007): Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health

Systems. In Proceedings of the 2nd International Conference on Availability, Reliability and Security, (ARESO˜07), Vienna, Austria. IEEE Computer Society, Apr. 2007.

[15] Emuoyibofarhe, O. J. (2012). E-Health/Telemedicine Readiness Assessment of some Selected States in Western Nigeria. International Journal of Engineering 2, (2) 1-7.

Authors' Profiles

Ifeoluwani, Jenyo holds a Bachelor of Technology (B. Tech.) degree in Mathematics / Computer Science and a Masters of Technology (M. Tech.) degree in Computer Science. Her areas of interest include telemedicine and mobile computing. She can be reached by phone on +2348060050863 and through E-mail on jenyoifeoluwani@gmail.com.

Elizabeth A. Amusan is currently a Senior Lecturer at the department of Cyber Security Science, Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria where she teaches and does research. Her areas of research interest include Information Security, e-Health, Telemedicine, Data Science and Mobile Computing. She is an active participant in collaborative research and a member of the Nigeria Computer Society (NCS). Dr. E.A. Amusan has several peer-reviewed articles in reputable national and international journals as well as referred conference proceedings.

Justice O. Emuoyibofarhe is a Professor in the department of Information Systems at Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria as well as the Pioneer and current Dean, Faculty of Computing and Informatics of the same institution. Prof. J.O. Emuoyibofarhe is also the Head of the Mobile and e-Computing Research Group, LAUTECH, Ogbomoso.

How to cite this paper: Ifeoluwani Jenyo, Elizabeth A. Amusan, Justice O. Emuoyibofarhe, "A Trust Management System for the Nigerian Cyber-health Community", International Journal of Information Technology and Computer Science(IJITCS), Vol.15, No.1, pp.9-20, 2023. DOI:10.5815/ijitcs.2023.01.02