CSEAN
CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA

Cyber Secure Nigeria 2019 Conference

April 9 – 11, 2019

Securing Electronic-Health Record Systems Using Cryptographic Techniques

Shefiu Olusegun Ganiyu[1], Olayemi Mikail Olaniyi[2], and Orooniyi Tosin[3]

Federal University of Technology Minna, Niger State, Nigeria
[1]shefiu.ganiyu@futminna.edu.ng, [2]mikail.olaniyi@futminna.edu.ng, [3]orooniyi.tosin@st.futminna.edu.ng

Abstract: The successful storage, manipulation and retrieval of electronic medical records are some of the important functions of Electronic-Health Record (EHR) Systems. More so, the confidentiality and integrity of health information is of paramount importance to healthcare management organizations. Unfortunately, the occurrence of information security breaches with regards to EHR, which include loss of valuable data as a result of theft by unauthorized users, is increasingly becoming worrisome situations. Furthermore, these security challenges have led to cases of intentional or unintentional disclosure of vital patients' information among others. Interestingly, previous studies attempted to implement secure systems in domains like finance, communication and commerce using asymmetric or visual cryptography. However, based on reviewed literatures, this security techniques are yet to be combined and applied as worthwhile approach to address authorization challenges in the EHR domain. Thus, a prototype web-based e-health record system was developed and combination of asymmetric and visual cryptographies were incorporated into the system as authorization mechanism to ensure confidentiality and integrity of pertinent health information. Subsequently, the fortified E-health record system provided important functionalities of a typical EHR record system, as well as prevent unauthorized users from accessing vital information.

Keywords**:** Heath record; Electronic-heath; Cryptography; e-health record system

I. Introduction

Electronic-health (e-health) is interchangeably used with Health Informatics, an interdisciplinary field that develops and applies theories, methods and processes for the generation, storage, retrieval, use and sharing of medical data, information, and knowledge (AMIA, 2019). One critical challenge of e-health is the issue of data storage through Electronic-heath Record (EHR), an electronic version of a patient's paper record. Characteristically, EHRs are designed to include the patient medical and treatment histories, diagnoses, medications, immunization dates, allergies, radiology images, and laboratory test results. They are also meant to provide secure patient medical information, only, to authorize users. However, sundry EHR's offer inadequate capacities to monitor or keep in check the exact health records to be shared, even with main family members and caregivers (Cushman, Froomkin, Cava, Abril, & Goodman, 2010).

Over the years, technology faces various modes of intrusion which include; the integration of incorrect data or destructive programs into information systems, theft resulting to loss of important data or programs from a system and overall takeover and manipulation of a system's set-up and performance. Usually, hackers carryout these security breaches as a means of satisfying their own agenda. More so, criminals use it to improve their own interests, as well as commercial organizations that utilize it as mechanisms for neutralizing rivals or terrorists whose attacks can spread over a wide geographical range, eventually producing related effects irrespective of the criminal (Onuiri, Idowu, & Komolafe, 2015).

Furthermore, the rate of information security issues with regards to Electronic-Health Records (EHR's) is increasingly becoming worrisome, this brings about the urgent need to mitigate these challenges so as to curb unauthorized manipulation, storage and retrieval of information, thereby, retaining required confidentiality, availability and integrity of the EHR's. Otherwise, any interception or interruption, may result to issues such as inaccurate diagnosis and medication, and in the worst case, death. Therefore, in this paper we present, a secure electronic health record using asymmetric and k of n visual cryptographies.

Visual Cryptography or Visual Secret Sharing (VC/VSS) is an information hiding technique that allows information (in form of images or text) to be encoded in a way that decoding is done by the human visual aid (Archana & Ambily, 2016). Developed by Naor and Shamir (1994), the technique involves sharing an encrypted secret image into n shares such that stacking a sufficient number of shares only reveals the secret image. In VSS, the shares generated contains only black and white pixels which makes it difficult to easily gain any information about the secret image by viewing only one share. The secret image is revealed only by stacking sufficient number of shares. (Basavegowda & Seenappa 2013).

Asymmetric cryptography otherwise known as public key cryptography is a data security technique, which uses two distinct keys in cryptographic process. Unlike symmetric cryptography that uses same key for encryption and decryption, asymmetric process includes generations of the two distinct keys (private and public) from complex mathematical algorithm. The public key is made available to all message senders for encryption purpose, whereas, the private key is reserved as secret and only known to the receiver (owner of the public key) for message decryption. While key generation is faster with symmetric cryptography, the reverse is the case with asymmetric cryptography. Nevertheless, safeguarding a key from unauthorised user during transfer among legitimate users is the main setback for symmetric cryptography, while such challenge does not arise in asymmetric cryptography.

Our contribution significantly provides a medium through which the privacy of a patient's electronic healthcare record could be preserved by enhancing the security measures on the EHR's since they are sensitive to patients and their caregivers. The remaining section of paper is organized into five sections. Section II provides review of related works, Section III presents the methodology, Results and discussion are presented in Section IV, while Section V concludes the paper.

II. RELATED WORKS

Harman, Flite, and Bond (2012) conducted systematic analysis of health management system. The authors highlighted numerous advantages of electronic system over manual approach to health management. Amongst others, the authors identified reduced storage space, physical security of records and delay in processing health information as major drawbacks of manual approach. However, the authors emphatically raised concern over security of patient information by healthcare handlers. Thus, Harman et al. (2012) suggested the use of encryption as a proactive countermeasure to ameliorate security of health information in terms of confidentiality for devices employed in processing and disseminating such crucial information. In a similar systematic review, Fernández-Alemán, Señor, Lozoya, and Toval (2013) agreed with Harman et al. (2012) on the major benefits of E-Health management systems and the importance of encryption scheme, but emphasised the need for more concerted efforts to address emerging security and privacy threats, because access to E-health systems becomes ubiquitous among stakeholders (Li, Zou, Liu, & Chen, 2011).

Likewise, Onuiri et al. (2015), explored various cyberspace challenges with respect to safeguarding information, investigating cyberspace threats, identifying stakeholders and transmitting information in E-health record system. The authors opined the combination of cryptography and biometric authentication as mitigating strategy for threats associated with e-health systems. Empirically, Qureshi et al. (2014) studied the effect of E-health which comprised of Telemedicine and mobile health on distant or remote locations. Interestingly, the authors stated the important characteristics of a successful and useful e-health system to include user-friendliness, easy-to-use and well-integrated functionalities, as well as a backup, tracking and alert facilities. The authors observed a tremendous shift in e-health adoption, but reported low adoption in developing countries due to inadequate information on e-health websites. Thus, Qureshi et al. (2014) proposed that a qualitative, secured and well-structured e-health system will enhance the operational efficiency and sustainability of the healthcare institutions.

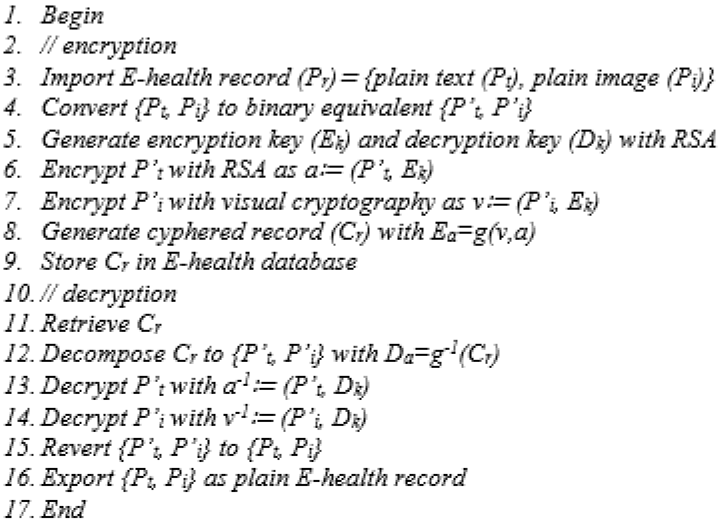
Also, Hawkes, Yasinsac and Cline (2000) analysed the possibility of securing financial documents with visual cryptography. The authors developed an application named VCRYPT which was described as a quick and uncomplicated visual cryptography technique. The VCRYPT is meant for privacy protection when data transits between offices, thereby preserving the integrity of document. According to Hawkes et al. (2000), previous visual cryptography systems suffered from the decoded images having a greying-effect or the deciphered image being blurry and much obscurer than the original image. Consequently, the VCRYPT application addressed this problem and also reduced the computational impact. Furthermore, in order to enhance the performance of visual cryptography irrespective of domain of application, D'Arco and De Prisco (2016) proposed the *deterministic* and *random grid models*. However, the authors reported issues relating to contrast, pixel expansion and randomness reduction in both models.

Recently, Okkali and Sandikkaya (2017) applied visual cryptography to facial recognition in surveillance system for privacy preservation. The system employed facial characteristics of targeted person is concealed and split into *n* shares which are put into distinct storage areas and under the control of distinct entities. More so, Kester (2013) developed a visual crytopgraphic encrytption system for medical image using pixel shuffling procedure. The system used algorithm that shuffled the red, blue and green (RGB) values of a pixel using an encryption key generted from the image. However, the system is limited to medical image which is only one of the the file formats involved in a comprehensive e-health record system. Again, Kester (2013) used same key for both encryption and decryption, which could expose it to key theft, a known problem with symmetric key cryptography. Again, Sugiharto et al. (2018) developed a crypto system that is based on visual cryptography and Rivest, Shamir and Adleman (RSA) techniques for only image encryption and decryption. Thus, the use of asymmetry cryptography (RSA) by the authors eliminates issues relating to security of key, yet the study is limited to image cryptography.

Accordingly, Harman et al. (2012), Fernández-Alemán et al. (2013), Onuiri et al. (2015) and Qureshi et al. (2014) focus on systematic review of visual cryptography in E-health management system without actual implementation of the security scheme in the domain. The studies revealed the stakeholders, core functions and security expectations of e-health record system. Although, D'Arco and De Prisco (2016) developed variants of visual cryptography mechanism towards performance improvement, but Hawkes et al. (2000) and Okkali and Sandikkaya (2017) applied the security techniques to other domains of human endeavour outside E-health record system. Perhaps, Kester (2013) was among few studies, which applied visual cryrptography to medical image, an aspect of E-health record system, but used symmetric cryptography and covered only image. Similarly, Sugiharto et al. (2018) utilised asymmetric technique, but their study is limited to image, while text data and specific domain of application were not considered.

III. METHODOLOGY

No doubt, visual cryptography is among the underlying techniques for guaranteeing security of images that concerns human visual system in digital space. Thus, this study utilised the algorithm proposed by Kester (2013) for medical image encryption. However, instead of generating encryption key from the image as implemented by the researcher, we use key generated by RSA for visual cryptographic. Also, RSA was used to secure textual data in the E-health record. One major advantage of this approach is that, the proposed system can leverage on the soundness of RSA for textual cryptography. Similarly, since typical E-health record comprises of both image and textual contents, then using asymmetric key for both contents will eliminate the need to have disparate encryption keys for a single cryptosystem. In addition, this approach promotes seamless integration and ciphering of text and image from system implementation point of view. Figure 1 shows the algorithm for the encryption and decryption processes, while Figure 2 presents the high-level diagram for same processes.



```
Begin
// encryption
Import E-health record ($P_r$) = {plain text ($P_t$), plain image ($P_i$)}
Convert {$P_t$, $P_i$} to binary equivalent {$P'_t$, $P'_i$}
Generate encryption key ($E_k$) and decryption key ($D_k$) with RSA
Encrypt $P'_t$ with RSA as $a := (P'_t, E_k)$
Encrypt $P'_i$ with visual cryptography as $v := (P'_i, E_k)$
Generate cyphered record ($C_r$) with $E_a = g(v,a)$
Store $C_r$ in E-health database
// decryption
Retrieve $C_r$
Decompose $C_r$ to {$P'_t$, $P'_i$} with $D_a = g^{-1}(C_r)$
Decrypt $P'_t$ with $a^{-1} := (P'_t, D_k)$
Decrypt $P'_i$ with $v^{-1} := (P'_i, D_k)$
Revert {$P'_t$, $P'_i$} to {$P_t$, $P_i$}
Export {$P_t$, $P_i$} as plain E-health record
End
```

Figure 1: Algorithm for E-health Record Encryption and Decryption

A. *System Architecture*

The system architecture for the proposed E-health record system is presented in Figure 3. The architecture shows the stakeholders, information flow and data storage, as well as the positions of security mechanism to ensure confidentiality and integrity of medical records. Most of all, the stakeholders are patients whose health information needs to be secured and medical team who is the custodian of the records. As indicated in the diagram, all stakeholders require appropriate asymmetric key to encrypt or decrypt desired information. Equally important, all stakeholders must pass authentication challenge by supplying valid username and password before accessing the system.

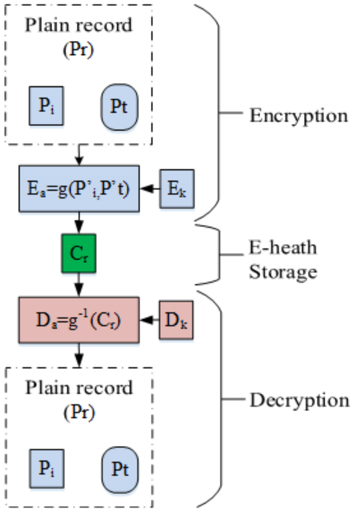


Figure 2: Encryption and decryption block diagram for e-health

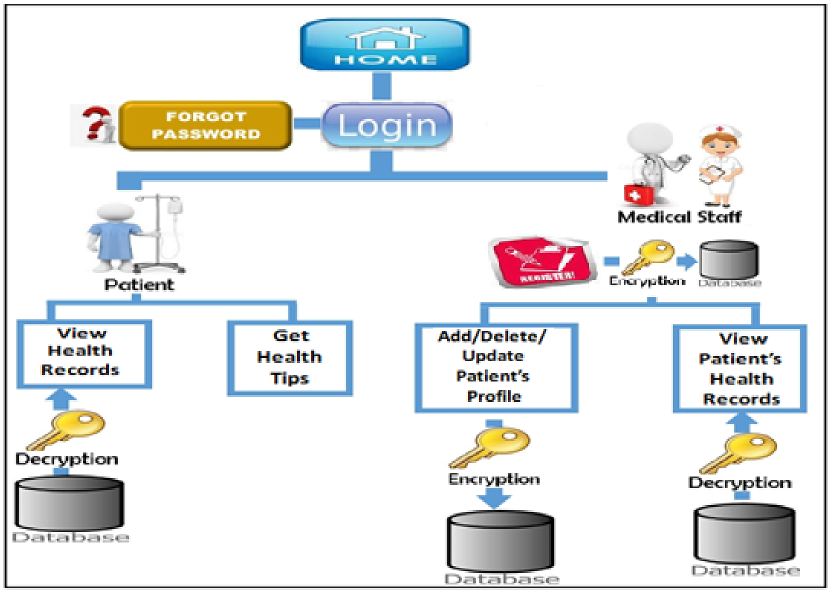


Figure 3: System architecture

B. *System Development*

The flow of information within the proposed system is presented in Figure 4. Thus, the flowchart guided the implementation of the system. Subsequently, the system was implemented as web application using Hypertext Preprocessor (PHP) platform and cryptography plugins. Then, MySQL database was used as database management system.

IV. RESULTS AND DISCUSSION

Figures 5 to 8 show some of the interfaces implemented for the E-health record system. For instance, all users are required to fill the form in Figure 5 as part of the sign-up process prior to login into the system. Thereafter, the interface presented in Figure 6 will be used for subsequent login by users depending on the role assigned to them at sign-up by system administrator. Again, Figure 7 depicts a typical health record for patient registered on the system. Similarly, Figure 8 reveals the access denial page displayed when user attempt to view health record with wrong access key.

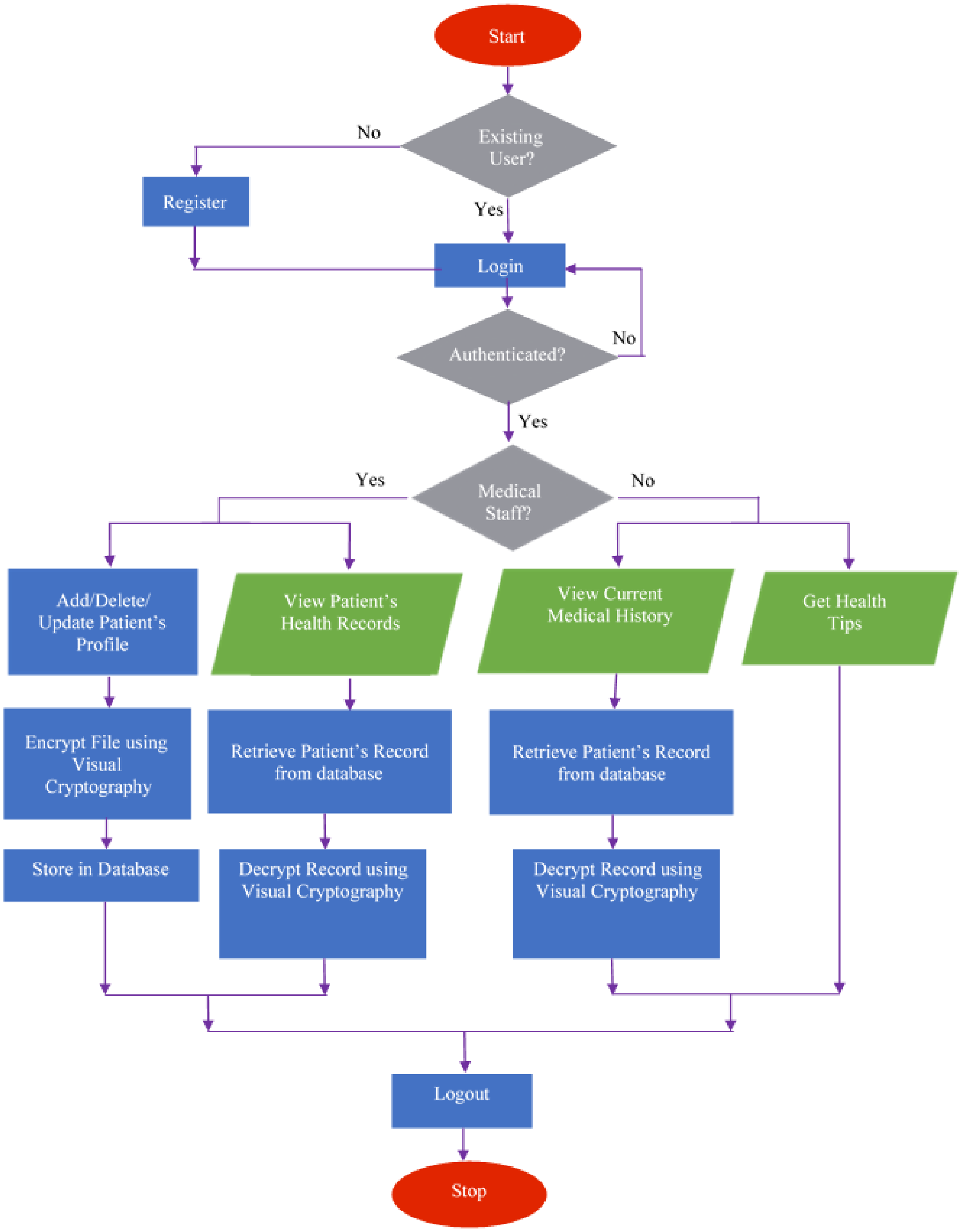
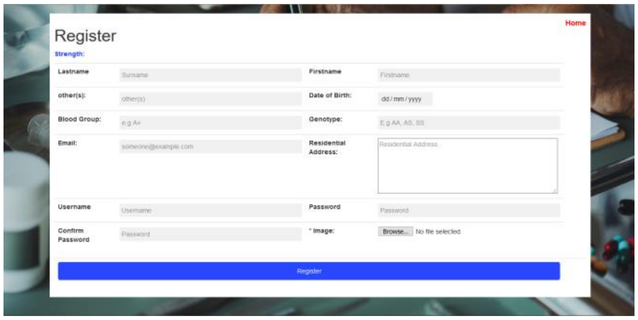

Start
Existing User?
No
Yes
Register
Login
Authenticated?
No
Yes
Medical Staff?
Yes
No
Add/Delete/ Update Patient's Profile
View Patient's Health Records
View Current Medical History
Get Health Tips
Encrypt File using Visual Cryptography
Retrieve Patient's Record from database
Retrieve Patient's Record from database
Store in Database
Decrypt Record using Visual Cryptography
Decrypt Record using Visual Cryptography
Logout
Stop

Figure 4: System flowchart

V. CONCLUSION

The synergistic combination of asymmetric and visual cryptography in the proposed EHR system has successfully provided a medium through which the privacy of a patient's electronic health record is maintained. This will no doubt ensure that patient's Electronic Health Records (EHR's) are securely stored and that only authorized persons are allowed to view them. It is still important that further studies be carried out to improve on the security of EHR's possibly by incorporating another security technique in addition to the Visual Cryptography technique. Also, quantitative evaluation should be conducted to measure the performance of the proposition in this paper.

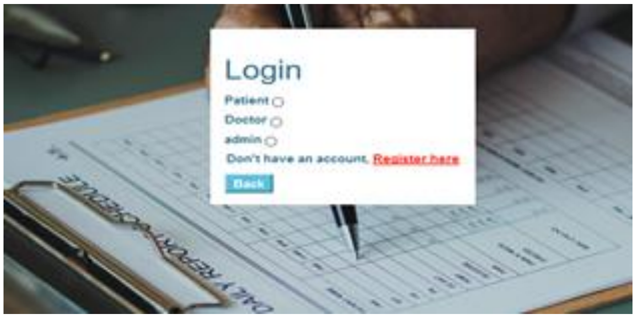


Register

Strength:

Lastname	Surname	Firstname	Firstname
other(s):	other(s)	Date of Birth:	dd / mm / yyyy
Blood Group:	e.g A+	Genotype:	E.g AA, AS, SS
Email:	someone@example.com	Residential Address:	Residential Address
Username	Username	Password	Password
Confirm Password	Password	* Image:	Browse... No file selected.

Figure 5: User registration



Login

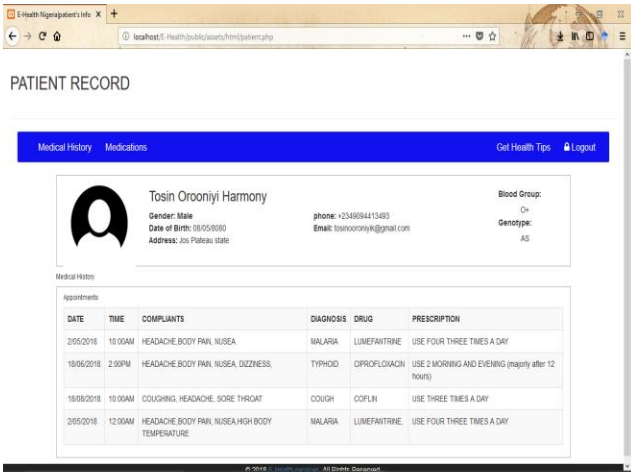
Patient ○

Doctor ○

admin ○

Don't have an account, Register here

Figure 6: User authentication



E-Health Nigeria|patient's Info
localhost/E-Health/public/assets/html/patient.php

PATIENT RECORD

Medical History
Medications
Get Health Tips
Logout

Tosin Orooniyi Harmony

Gender: Male

Date of Birth: 08/05/8080

Address: Jos Plateau state

phone: +2349094413493

Email: tosinooroniyik@gmail.com

Blood Group: O+

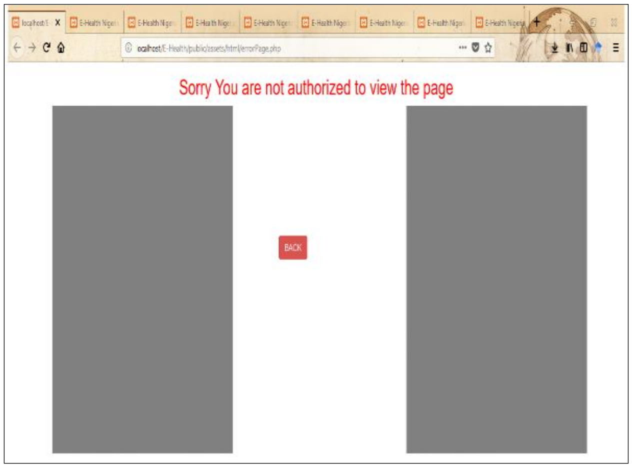
Genotype: AS

Medical History

Appointments

DATE	TIME	COMPLIANTS	DIAGNOSIS	DRUG	PRESCRIPTION
2/05/2018	10:00AM	HEADACHE,BODY PAIN, NUSEA	MALARIA	LUMEFANTRINE	USE FOUR THREE TIMES A DAY
18/06/2018	2:00PM	HEADACHE,BODY PAIN, NUSEA, DIZZINESS,	TYPHOID	CIPROFLOXACIN	USE 2 MORNING AND EVENING (majorly after 12 hours)
18/08/2018	10:00AM	COUGHING, HEADACHE, SORE THROAT	COUGH	COFLIN	USE THREE TIMES A DAY
2/05/2018	12:00AM	HEADACHE,BODY PAIN, NUSEA,HIGH BODY TEMPERATURE	MALARIA	LUMEFANTRINE,	USE FOUR THREE TIMES A DAY

Figure 7: Patient record



Sorry You are not authorized to view the page

Figure 8: Access denied due to wrong secret key

REFERENCES

AMIA 2019. AMIA Health Informatics Core Competencies Retrieved online at https://www.amia.org/AMIA-Health-Informatics-Core-Competencies-for-CAHIIM.PDFom on 14th March 2019

Archana, P. S., Ambily, O. 2016. Visual cryptography in internet voting for extended security. International Journal of Engineering Research and General Science, 4(2), 365–368.

Basavegowda, R., Seenappa, S. 2013, Electronic Medical Report Security Using Visual Secret Sharing Scheme, 15th IEEE International Conference on Computer Modelling and Simulation. 78-83

Cushman, R., Froomkin, A. M., Cava, A., Abril, P., Goodman, K. W. 2010. Ethical, legal and social issues for personal health records and applications. Journal of Biomedical Informatics, 43(5), S51–S55. https://doi.org/10.1016/j.jbi.2010.05.003

D'Arco, P., De Prisco, R. 2016. Visual Cryptography Models, Issues, Applications and New Directions. In Innovative Security Solutions for Information Technology and Communications (pp. 20–39). Springer International Publishing. https://doi.org/10.1007/978-3-319-47238-6

Fernández-alemán, J. L., Señor, I. C., Ángel, P., Lozoya, O., Toval, A. 2015. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Harman, L. B., Flite, C. A., Bond, K. 2012. Electronic Health Records: Privacy, Confidentiality, and Security. American Medical Association Journal of Ethics, 14(9), 712–719. Retrieved from www.virtualmentor.org

Hawkes, L. W., Yasinsac, A., Cline, C. 2000. An Application of Visual Cryptography to Financial Documents. Tallahassee.

Kester, Q. 2013. A Visual Cryptographic Encryption Technique for Securing Medical Images. International Journal of Emerging Technology and Advanced Engineering, *3*(6), 496–500.

Li, F., Zou, X., Liu, P., Chen, J. Y. 2011. New threats to health data privacy. In BMC Bioinformatics, 12, pp. 1–7.

Naor, M., Shamir, A. 1995. Visual Cryptography. Advances in Cryptology - EUROCRYPT'94, 1–12.

Okkali, A., Sandikkaya, M. T. 2017. Preserving Privacy Using Visual Cryptography in Surveillance Systems. In (UBMK'17) 2nd International Conference on Computer Science and Engineering, pp. 1141–1144.

Onuiri, E. E., Idowu, S. A., Komolafe, O. 2015. Electronic Health Record Systems and Cyber- Security Challenges. In International Conference on African Development Issues pp. 98–105.

Qureshi, Q. A., Khan, I., Shah, B., Nawaz, A., Waseem, M., Muhammad, F. 2014. E-Health System: A Study of Components and Practices in Developing Countries. Developing Country Studies, 4(16), 119–126.

Sugiharto, B.S., Kurniasih, N., Abdullah, D., Iswara, I.B., Napitupulu, D., Laritmas, S., Mouw, E., Ahmar, A.S., Kurniawati, N., Rahim, R. 2018. Visual Cryptography with RSA Algorithm for Color Image. International Journal of Engineering & Technology, 7 (2.5), 65-68.