A METHODICAL REVIEW OF SECURITY AND PRIVACY ISSUES IN CLOUD-BASED ELECTRONIC HEALTH RECORDS

Oladotun Olusola OKEDIRAN
Department of Computer Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
ookediran@lautech.edu.ng

Keywords: access control, cloud, electronic health records, model, privacy, security, vulnerability

Abstract: *Electronic Health Records (EHR) has emerged as a significant alternative to paper-based health records. Today, EHR is a model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. Nevertheless, there are high security and privacy concerns as data available on cloud-based EHR could be exposed by these third party cloud repositories and accessed by unauthorized parties. Many schemes and models that were based on biometrics, blockchain, watermarking, steganography, Transport Layer Security/Secure Sockets Layer (TLS/SSL), Role Based Access Control (RBAC), Discretionary Access Control (DAC), Mandatory Access Control (MAC), Cipher text policy Attribute Based Encryption (CP-ABE) and other encryption models have been proposed to secure and ensure privacy of patients 'data on cloud-based EHR. Each of these security and privacy protection schemes/models has their significant advantages and attendant shortcomings. In this paper, a methodological review of literature on various schemes and models proposed for proffering solutions to security and privacy of patients 'data on cloud-based EHR was carried out. A total of ninety-five research articles were reviewed with the models or schemes employed for securing and guaranteeing privacy of electronic health data highlighted. Also, their strong points and drawbacks were elucidated. The reviewed articles were trimmed down to the forty-two presented in this paper based on similarities identified in the models or schemes implemented by some authors and/or relevancy of article's title. Remarks and recommendations were made regarding the review and future directions on security and privacy of cloud-based EHR were also suggested.*

1. INTRODUCTION

Documentations of health records of patients in many counties are still predominantly paper-based. However, these paper-based health records are not scalable in terms of storage, prone to error, insecure, susceptible to damage and degradation over time, highly unavailable, time consuming in accessing, no visible audit trail and version history and may generate an extensive paper trail to mention but a few. Consequently, there was a great interest in migrating from paper-based health records to EHR. Initially, this interest was primarily from individual healthcare facilities; but later, propositions for implementation of EHR were for an integrated health records system. Today, with the increasing rate of the adoption of cloud computing approaches in the health sector of some countries by a substantial number of healthcare facilities, cloud servers are now remote repository of such integrated health records system.

This health records system is accompanied by the following advantages: improved medical documentation and patient service, enhanced efficient and effective clinical workflows, improved medication management, and reduced transcription and labor costs [1]. Accompanying these benefits of integrating health records, however, are issues bothering on security and privacy threats, due to advances in information and communications technology [2].

According to [3]; [4], there are three aspects of security, which are confidentiality, reliability

and availability. The definitions of these three are summed up in [5]; [6]; [7].

i. Confidentiality is the process that ensures that only the entitled users, under the defined terms, have access to the information.
ii. Reliability is of two sides; integrity, which refers to a course of action that guarantees that information content has not been modified, forged, deleted without detection, and authentication which is the verification that the ownership of information is actually due to the right patient and it emanated from the expected source.
iii. Availability is the property of being useable and accessible upon demand by entitled users under the defined terms of access and exercise.

Security needs vary from one application to another and the privileged aspects they emphasize. In the health sector, to meet security requirement, three characteristics should be ensured: confidentiality, integrity and availability [3] and [8]. Summarily, health information must be preserved from unauthorized access, its contents protected to ensure patient safety and be readily available for access and use by authorized user even in the face of eventualities such as system failures, malware attacks, cyber attacks and natural disasters.

Health information contains highly private contents of the personal information for a patient, which means they are closely related to patients' privacies and hence should be kept with upmost secrecy. Privacy is the denial of access to information (that is access control) by unauthorized individuals. Westin in [9] defined privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Risks and threats to security and privacy of EHRs can be classified into two categories which are innocent manipulations and malicious ones [10]; [11]. The former includes accidental losses or theft of sensitive clinical data. The later involves the human factor which makes it complicated to assert the extent of malicious intents. However, malevolence is usually articulated under the captions that include: hacking, virus infection, targeted logical attacks, disclosure, embezzlement or immaterial assets alteration and so on [12]. The knowledge of the security and privacy characteristics that EHR possess could be vital if these risks and threats are to be confronted and mechanisms to increase the security of data of EHRs are to be adopted.

In proffering solutions to the risks and threats to security and privacy of cloud-based EHRs, different approaches that were based on cryptography watermarking, steganography and so on, have been proposed and implemented to ensure the preservation of security and privacy of cloud-based EHR data. In this paper, a methodological review of selected literatures on security and privacy solutions to cloud-based EHR data was carried out with the technique employed outlined and their strong points and drawbacks elucidated. The rest of the paper is detailed as follows: the methodology is presented in Section 2 while Section 3 contains the review of selected literature. Section 4 concludes the paper and references are listed in Section 5.

2. METHODOLOGY

The review of literature carried out in this paper attempted to collect relevant empirical evidences pertaining to security and privacy issues of EHR in order to assess the techniques proposed or implemented and evaluate them critically and to draw inferences on the reviewed research works. It may be noted however, it is impractical to carry out a review of all literatures available that relates to security and privacy of EHR. The study selection criteria employed in this work is stated in sub-section 2.1.

2.1 Study Selection Criteria

The sources of the reviewed articles of this paper spans databases that include IEEE explore, ACM, Elsevier, Science Direct, Springer digital Scopus and PubMed, databases. Also, articles pertaining to the subject matter were downloaded from other journals that are not in the same ranked as those earlier mentioned. The keyword/phrases used in selecting these articles are:

i. EHR
ii. Security and privacy of EHR in cloud
iii. E-health and cloud technology/computing
iv. Framework for cloud-based e-health

v. Cryptographic Approaches for securing EHR

Using the aforementioned keywords/phrases, the search found more than 120 articles. Some of the articles found by the search were filtered out due to similarities in model/schemes implemented and authorship thereby remaining 95 articles. Another 53 articles were left out after a study of the relevancy of the title of the articles based on their abstract. The remaining 42 articles are presented in the final review.

2.2 What are EHR?

EHR is a documentation of health-related information about an individual with the primary aim of being a reference for consultation by medical practitioners for patient care. More technically defined, a EHR is an electronic version of a patient's medical history, that is maintained by the provider over time, and may include all the key administrative and clinical data relevant to that person's care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports [13]. The benefits of this include improved medical documentation and patient service, enhanced efficient and effective clinical workflows, improved medication management and reduced transcription and labour costs [1].

2.3 Requirements for Security and Privacy in EHR

In today's healthcare, EHRs have been implemented in some countries to facilitate healthcare providers, insurance firms and patients themselves to create, manage and access health data of patients from anywhere and at any time. While it is convenient to have EHR services deployed via cloud, there are associated risks bordering on security and privacy of health data which could prevent its extensive adoption. Denial of Service attacks (DoS), collusion attacks, spoofing, man-in-middle attacks, cloud malware injection attacks [14] are imminent attacks in most cloud-based EHR systems.

In many countries whereby EHR have been implemented, there are instituted requirements on the security and privacy of health information. For instance in the United States, it is the Health Insurance Portability and Accountability Act (HIPAA). The essential security and privacy requirements of for electronic information are [14]:

i. *Confidentiality:* Patient health information should be protected from individuals who should not have admittance to it.
ii. *Data integrity*: This requirement guarantees that modification, forgery or deletion of health information is absolutely forbidden. Therefore, shared health information must be an accurate version of the original information without any form of revision or adjustment.
iii. *Non-repudiation:* This implies that a medical practitioner should not be able to refute any activity he/she performed on a patient health data. Any activity carried on patient health information must be provable.
iv. *Authenticity:* The requirement that ensures that only authorized and certified should be accessible to health data.
v. *Auditing:* This ensures that health data should be constantly and consistently monitored together with the type of activity to guarantees the protection and security of such data. This aid users to ascertain the confidential status of his/her data.
vi. *Accountability:* The responsibility to be liable to and substantiate personal or collective actions and resolutions.
vii. *Anonymity:* requirement that guarantees the secrecy of the identity of the subject in a manner such that the identity of stored health data cannot be accessed by the cloud servers.

2.4 Overview of Cloud Computing

Cloud computing is a computing paradigm, where a large collection of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage [15]. From a user perspective, it is a subscription-based service where users can obtain networked storage space and computer resources [16]. Cloud

servers come in three variants: trusted servers, semi-trusted servers and untrusted servers [14]. A trusted server is one that has complete reliance in which no information stored can be leaked or threatened by internal adversaries. On the other hand, semi trusted servers are modest but questionable servers that acquire health data by conspiring with malevolent users while untrusted servers are servers that cannot be trusted; they are without any security and privacy preservation modality and are susceptible to attacks from both within and without [17]. Architecture of cloud-based electronic health data is depicted in Figure 1.

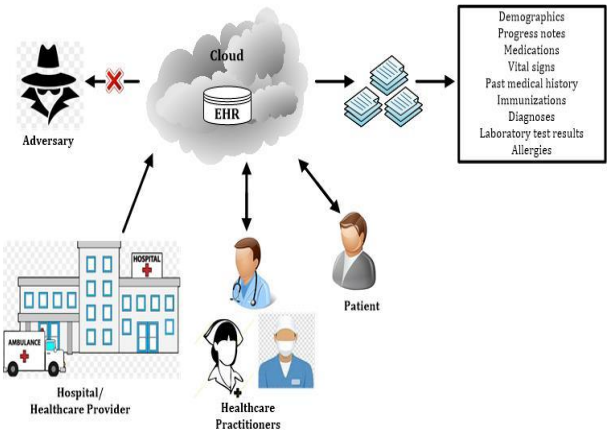

Figure 1: Architecture of Cloud-based Electronic Health Data

3. LITERATURE REVIEW

Li *et al.* in [18] proposed an Attribute Base Encryption (ABE) security scheme for security and ensuring privacy of patient data. The proposed scheme by the authors minimizes the intricacy the may occur due to key distribution. However, patient-defined access control strategies are not expressly supported by the scheme.

Also, in [19], the authors proposed a RBAC security model which is simple and expedient for deployment of security and privacy strategies on sensor networks. The drawback of the model is that there is no access control mechanism to prevent unauthorized usage in emergency situations.

Zhu *et al.* in [20] proposed a biometric identification model for proficiently ensuring privacy wherein a large amount of biometric data that includes facial patterns, voice patterns, irises and fingerprints are encrypted and outsourced to a cloud in other to circumvent pricey computation and storage costs. The model proposed by these authors can resist collusion attacks and guarantees a very high level of data privacy. An area of application of this model is data storage in cloud-based e-health systems whereby encrypted and stored health data can achieve a confident level of data protection. This model is however found wanting in terms of security level, as sensitive health data is bared to database proprietors. Furthermore, the model cannot be used in EHRs as it is not patient-centric and extremely computationally complex; hence impractical for real life situation.

In [21], the authors proposed a hybrid multi-authority CP-ABE access control strategy that is robust and verifiable using a combination of *(t, n)* threshold secret sharing and multi-authority CP-ABE scheme for data storage in public cloud. The strategy proposed by these authors is of enhanced performance and security, overcoming the single point constriction problem. Also, Xue *et al.* in [22] developed a robust and efficient access control strategy that proffered solution to the single-point performance constrictions in the majority of the obtainable CP-ABE proposals and implementation by utilizing an auditing system. Although the strategies proposed by these authors in [23] and [24] are highly secured access control strategies, they cannot be implemented in e-health infrastructures because are they are pivoted on Central Authority and multiple Attribute Authorities and hence susceptible to attacks by insiders.

Explicit literature search reveled that a large majority of obtainable cloud-based data storage systems with proven security mechanism often suffers of reliable access control mechanisms, attracts performance operation cost and does not support dynamic user management. Wei *et al.* in [23] proffered solution to this problem by developing a cloud-based secure data storage mechanism based on reversible storage Identity Based Encryption (IBE). Nevertheless, the mechanism developed in this work is not scalable and key authority can be compromised.

Also, in [24], the authors evaluated different encryption based approaches for realizing integrity and confidentiality of electronic health data. The evaluated encryption approaches include cipher algorithms such as

RC4, Advanced Encryption Standard (AES) and so on. The results of their evaluation showed that the reliability of some ciphers is not fail-safe.

In [25], the authors proposed an attribute based and security guaranteed cloud storage system. The system strong points include data privacy protection, dynamic user management, anonymity of non-traceability of data provider, scalability and fine-grain access control. The major shortcomings of this system are the complexity in bilinear pairing computations and high data latency leading to high cost of data decryption.

A symmetric cryptographic key management protocol was proposed by Lee and Lee in [26] to fulfill the requirements stipulated in Health Insurance Portability and Accountability Act (HIPAA) guidelines. In the protocol, three distinctive entities which are government healthcare office, server of a healthcare provider and patients are used while three phases of the protocol include registration, encryption and decryption. The process of usage of the protocol is initiated with patient registration with government healthcare office in order to obtain a healthcare card and hence validating such a patient for medical services obtainable at the healthcare provider. The next phase of operation of the protocol is encrypting the Protected Health Information (PHI) via the activation of the health card by biometric or PIN authentication. This phase can be accomplished by concatenating the hash value of patients' master key and the session key of healthcare provider to generate a session key and cryptographic checksum. The last phase which is the decryption is carried out in two ways which one, with the approval of the patient and two, other with cases of emergency. This can be accomplished by computing the master key and session key of the healthcare provider.

In another model for proffering solutions to security and privacy issues of health data, Guo *et al.* in [27] proposed a distributed but collaborative framework for authentication and authorization processes for electronic health data. The framework proposed by the authors allows for both patients and medical practitioners to carry out these two processes. Furthermore, the framework catered for security, privacy and variability of the attributes of all users. The major disadvantage of the framework is that it is not interoperable; sharing of medical data across different domains is not possible.

Another scheme proposed by Kumar *et al.* in [28] was based on an encryption framework built on ABE for securing electronic health data. The principal merit of the approach is the ability to handle key management complexities. Nevertheless, the approach proposed by the authors is not flexible and scalable.

Chi and Lei in [29] presented a unique encryption technique, the Deniable ABE scheme that was founded on Waters CP-ABE scheme which permits cloud storage donors to generate forged user secrets from cipher text that was stored in cloud to prevent the data from obliger on the outside. The technique presented in this work blends the merits of ABE and symmetric key encryption as a multi-privileged access control for EHRs by merging the encryption of data from multiple patients, similar to the scheme proposed by Li *et al.* in [30].

Zhang *et al.* in [31] presented a model that efficiently predicts diseases while ensuring patient privacy. This model was based on Single layer Perceptron learning algorithm. Symptom information submitted by patient are encrypted by the model and this encrypted information and the encrypted prediction models trained by cloud is utilized in patient diagnose of the disease with patient privacy preserved in the whole process. The technique and model presented by the authors in [30] and [31] respectively guarantees a top-level data privacy, but they are computationally complex and there inherent issues of scalability in implantation, hence they are impractical for securing and ensuring privacy in health records.

Zhu *et al.* in [32] underlined the need for securing electronic health data by developing a framework that utilizes re-encryption and ABE with proxy encryption built on Rivest Shamir and Adleman (RSA). In the framework, write license keys are authorised only for medical practitioners while the read license keys are given to patients. The benefits of the framework proposed by the authors includes; reduced computational cost, restrictions on access to patient data by medical practitioners without due approval by patients and so on. However, the main demerit of the framework is limitation on number of users that can be catered for.

In [33], the authors, Sunagar and Biradar developed a security approach that encrypts patients 'information in a cloud environment using AES. The framework proposed by the authors is believed to be highly secured and guarantees data privacy but it is operation system dependent in terms of implementation. Furthermore, the framework is complex to realise in practise.

Also, Bahtiyar and Caglayan in [34] from the perspective of an entity proposed a model for securing electronic health services that utilizes a trust-based assessment methodology. An essential component of the model is an architecture which provides a distinctive trust assessment that can be used to evaluate a defined quality of a security system. The simulation results of their work proved that the proposed model outperformed other trust models developed for e-health solutions in terms of trust computation. On the other hand however, the model is not explicitly stated as the values of some mathematical variables used in the model were not evidently evaluated.

A hybrid scheme comprising of Multi-authority ABE (MA-ABE) and AES was presented by Shrestha *et al.* in [35] for access control, security and privacy in an e-health system. Furthermore, the scheme presented by these authors improves scalability, safeguards the e-health system from potential attacks that include, eavesdropping, DOS and man-in-the-middle attacks.

Although many anonymization approaches have been proposed in literature by many researchers, one major challenge associated with most of this approaches is the considerable delay in the course of the anonymization process. The reason for this is not far to seek. Most of these works attended majorly to the application of security strategies to data acquired from data streams. This shortcoming of anonymization approaches was however addressed by Kim *et al.* in [36]. The authors developed a delay-free anonymization for protecting and ensuring the privacy of electronic health data. There was no time delay in the approach developed by the authors since data streams are anonymized instantaneously with phony values. Furthermore, delayed validation was also promoted to improve data functionality of the anonymization outcomes while simultaneously managing the phony values. The main disadvantage of the approach is that consideration was not given to the statistical analysis hampering the reliability of results of anonymization. Also, the timing for the late validation wasn't investigated by the authors.

Chen *et al.* in [37] proposed a security and privacy preserving approach to secure health record in regular and emergency conditions in a hybrid healthcare cloud. The proposed approach encrypts every individual medical record using a personal symmetric key *ck* with a symmetric cipher both in public and private cloud environments. The patient health record which is to be created by the doctor is encrypted with *ck* together with a license *L*. Access to the encrypted data is granted to the cloud by the license *L* via an emergence key which it provides, even in situation whereby direct access to the server is denied. Decryption of patient's EHR is carried out by the doctor and this is accomplished via the smartcard provided by the patient. This approach proposed by these authors requires that all medical records be encrypted and the process of decryption can only be carried out using the patients' private keys which is essentially of two parts. One part of the key is secured on the hospital server while the other part is stored on the smartcard of the patient. However, the main shortcoming of this approach is the need for the encryption of the license file with the public key of the hospital.

Karakis *et al.* in [38] attempted to secure vital health information by proposing a methodology that combines health data into a solitary file using image steganography. The authors proposed two image steganographic techniques that relies on similarities and fuzzy logic with the aim of selecting the non-sequential least significant bits (LSB) of image pixels. The authors in this work achieved gray levels in the pixels that hide the message by using similarity values. The method as proposed by the authors secures the information and prevents all types of attacks by symmetric ciphers and lossless compression. The disadvantage of this approach is that noise cancellation is not within its scope and embedding capacity cannot be improved since data reduction was not catered for.

It was highlighted by Kester *et al.* in [39] that electronic health based information must be secured and its privacy preserved. Towards this end, these authors considered the reversal of encrypted and watermarked images in order for

plain images that was encrypted and watermarked to be absolutely reversible because of the sensitivity of the information content of medical images. The authors suggested a recoverable watermarked and encrypted image processing methodology for security and privacy of medical images. The limitation of this method however is that only medical images are the application area; audio and text data were not considered.

In an effort to secure the exchange of electronic health data over open communication networks, Simplicio *et al.* in [40] implemented a framework that was used to present a SecureHealth architecture founded on Transport Layer Security/Secure Sockets Layer (TLS/SSL). SecureHealth is an architecture that provides security services such as authorization for stored and transmitted data. It has the advantage of preventing unauthorized access to health information in systems in which it is deployed. In spite of the merits that accrue from this framework, the major disadvantage is that it is not scalable and it is platform dependent. For cloud based systems, there must be opportunity for scalability and future expansion.

Efforts were made by the authors in [41] to ensure security and privacy of information in an e-health infrastructure. These authors proposed the implementation of a dual level-key access control and zero-knowledge protocol. The protocol guarantees secure connections amongst entities using DUKPT and a dual-level combination of key encryption. A performance analysis of the scheme premised on its capacity to resist attacks and confidentiality of data showed that the scheme can withstand a fairly large number of concurrent requests for authorization with an exceptional response time. However, the scheme was found wanting in that it is restricted in entities number. This means it is not scalable. It's therefore not suitable for a cloud-based environment because of its inability to allow for collaborative resource sharing.

Gajanayake *et al*. in [42] designed and implemented an access control scheme for securing and enhancing privacy of e-Heath data. The scheme was realised by fusing three different security strategies which are: RBAC, MAC and DAC. This resulted in a scheme in which patients and medical care providers can state and set access privileges, though the scheme is limited in its applicability as it is strictly a standalone security scheme.

Also, Rezaeibagha and Mu in [43] designed and implemented an access-control model to proffer solution to the problem of security and privacy in EHR. The model developed by the authors utilized access control policy transformation and a hybrid cloud framework to provide a failsafe authorization and access control in electronic data exchange amongst diverse healthcare providers. The model is however disadvantaged, because it is not scalable as there is a limit to the number of allowed users.

Over the years, it has been proven that the unilateral application of cryptographic schemes for securing data is not foolproof. In consonance with this assertion, Sahi *et al.* in [44] carried out a systematic review of selected security models and approaches proposed in literature to secure electronic health data and preserve their privacy. Based on the inferences drawn from their review, the authors proposed a two-way approach to secure and enhance privacy of electronic health data. The first approach is a Security-Privacy guaranteeing approach and the second, a failure recovery approach. The first approach is an efficient means of realizing security requirements for privacy and integrity; while the second approach ensures a reliable authentication mechanism for electronic health data. The key drawback of this work however is that the two approaches are interdependent; if one is non-functional, that other too will not be functional. Furthermore, this security model is non-interoperable to the level of being implemented in a cloud-based infrastructure.

Chen *et al.* in [45] proposed a security model that was based on Lagrange interpolation polynomial to create a secure personal health record information access which is duly scaled for huge number of users. The model employed a cipher based on Lagrange multipliers for the encryption of health records by making certain that every patient has utmost control over their medical records. Since key generation can be accomplished by individual patient, therefore, who or whom they share their health records with is at their discretion. Hence, the complexities of managing key are greatly minimized; thereby maximizing access control rights of patients and further permits the issuance of restricted access to medical practitioners and

researchers. However, this security model is computationally expensive.

Percarina *et al*. in [46] proposed an architecture termed SAPPHIRE, which was based on the hybridization of RSA and AES in an attempt to preserve the privacy of users by catering for anonymity and improving the policy administration for the principal data owner. Also in [47], the authors attempted to secure the storage of EHR by presenting a hybrid cipher technique. The authors proposed using Blowfish algorithm to encrypt health data and an enhanced RSA for keys encryption. The technique provides an enhanced security than a unimodal encryption technique.

In [48], the authors developed a hybrid scheme for the security and privacy preservation of patient data by fusing ABE and image steganography for the insertion of encrypted doctor's prescription and then onward transmission to pharmacist. Similarly, in yet another hybrid security system for integrated health records in cloud-based e-health infrastructure, the authors in [49] hybridized AES and Key Policy ABE (KP-ABE). The AES component of the hybridization was deployed for file encryption for uploading into the e-health cloud while KP-ABE was devised for the provision of users access privileges related to their attributes.

In [50], the authors proposed a cloud-based e-health dynamic access control mechanism termed risk aware task-based control which only grants access to user based on the three basic data security requirements, that is availability, integrity and confidentiality.

The authors of [51] developed a secure framework which partitions electronic health data into many segments. Individual segments are encrypted by a private key cipher and then stored in a transposed mode by another cloud provider. The data order and process of decryption process is in the knowledge of the user. This mechanism guarantee's security and secrecy of data and it is adaptable to all manners of security scheme employed by the cloud provider.

Sharma and Balasubramanian in [52] utilized a biosensor data of the patient to develop a framework for securing health monitoring application. The developed framework catered for data security and ensures secured access to the data at all times in storage and sharing via the cloud.

Also, in [53], the authors developed a secure but decentralized architecture for an e-health system which they called *iMedikD*. The architecture was developed to proffer solutions to the attendant problems of link failure and low/no fault tolerance that plagues centralized web-based e-health systems.

The authors of [54] suggested an architecture for securing and preserving patient privacy using a dual-level mechanism consisting of Mandatory Access Control Security Model (MACSM) and Access Control List Security Model (ACLSM). The architecture is expected to be of high fidelity, efficiency and reliability in securing patient's data.

Albarki *et al.* in [55] proposed a protocol that is robust and secured for remote user over open communication channels. The protocol guarantees secure communication between patients and doctors and preserves users' identity via a permutation of biometric authentication, passwords and smart devices.

Okediran in [56] proposed a security scheme for preserving patient information privacy in digital medical imaging. The scheme entails partitioning medical image that are in a medical imaging standard format, the Digital Imaging and Communications in Medicine (DICOM) into two: the medical image and patient's met-data. The meta-data is encoded (using UFT-8 character encoding), encrypted (using a public key cipher, ElGamal) and then embedded in the Region of Non-Interest (RONI) (using a discrete cosine transform based methodology) of the other component of the partition, the medical mage. The results of the performance evaluation of the scheme indicated that it is very secure, robust and the hidden patient data, highly imperceptible.

Similarly, Okediran in [57] developed a hybrid crypto and watermarking system for securing the transmission of medical images over open communication system. The crypto component of hybridization is the fusion of an asymmetric cipher, the Rivest-Shamir-Adleman (RSA) algorithm and a symmetric cipher, the Rivest Cipher 4 (RC4) algorithms while Spread Spectrum techniques (Direct Sequence and Frequency Hopping) were employed for watermarking. The evaluation results of the performance of the system showed that the

system is secure, utterly revertible, robust and highly imperceptible.

Han *et al.* in [58] proposed an architecture for a secure health information storage system based on blockchain technology. The proposed architecture provides a tamper-proof reliable storage services. Furthermore, data validation time is greatly reduced. However, the cost of deploying this architecture is on the high side. Similarly, in [59] Cao *et al.* developed a cloud-assisted secure e-health system for tamper-proofing electronic health records using blockchain. The developed system is proven by the authors to be highly efficient in providing security, tamperproof and does not need a Central Authority. However, more research needs to be done to verify these claims and on blockchain to improve its security concepts.

In [60], the authors proposed a novel data sharing and management scheme that gives authorization to patients over their health records based on the security and privacy advantages of blockchain and Access Verification and Permission Announcements (AVPA) smart contracts. The scheme proposed in their work gives authority to patients over their records and it curtails the reliance on record generating institutions; patients are allowed to discriminatory share their records and divulge specific fraction of it with particular data-users leveraged on the desired privacy preferences. The security analysis carried by the authors showed that shared patient data can be protected against various potential threats. It may be noted however, that AVPA smart contracts are usually very complex based on the number of computations and their corresponding complexity, hence posing as the major disadvantage of this work.

4. CONCLUSION

The advantages of digital healthcare cannot be overemphasized. However, the mainstream of data in this type of healthcare system is cloud-based, therefore, there is a dire need to secure them from unauthorized access because they are susceptible to threats and breaches. Most of the seurity solution for this healthcare system only guarantees a defined level of invulnerability, but certainly not a foolproof assurance. Therefore it is imperative to have a research breakthrough in this context

In this paper, a methodical review of literature on security and privacy issues in cloud-based EHR was carried out. A total of ninety-five research articles were reviewed but trimmed down to forty-two based on similarities identified in the techniques implemented by some authors and/or relevancy of article's title. The techniques employed for securing and ensuring privacy of electronic health data in storage, sharing and transmission were highlighted. These techniques varies from cryptograhic, non-cryptographic, steganography, blockchain, watermarking and biometrics. In some instances, some authors featured more that one of the aforemention techniques. Also, the strong points and drawbacks of these techniques were elucidated.

The drawback(s) identified for each technique can be considered as existing open problems and can suffice for future research in deriving an improved security strategy than the previous version of the technique. Fuurthermore, this paper can also serve as a reference guide to other researchers developing security standards for cloud-based EHR or e-health systems.

5. REFERENCES

[1]. Burk D., "*A framework for sharing personal medical information securely and efficiently across public / private institutions*", Cisco Internet Business Solutions Group (IBSG), 2010. Retrieved from http://tools.cisco.com

[2]. Farzandipour M., Sadoughi F., Ahmadi M., and Karimi I. , "*Security requirements and solutions in electronic health records: lessons learned from a comparative study*". Journal of Medical Syst ems 34(4):629–42, 2010.

[3]. Allaert F. A. and Dusseire L., *"Security of health system in France: What we do will no longer be different from what we tell?*, International Journal of Biomedical Computing. 35(1):201-204, 1994.

[4]. Coatrieux G., Maitre H., Sankur B., Rolland Y. and Collorec R., *"Relevance of watermarking in medica imaging"*. In: Proc. IEEE Conference on Information Technology Applications in Biomedicine, Arlington, USA, pp 250-255, 2000.

[5]. Armoni A., *" Healthcare information systems: challenges of the new millennium"*. Idea Group Inc (IGI), 2000.

[6]. Jennett P., Watanabe M., Igras E., Premkumar K. and Hall W., *"Telemedicine and security. Confidentiality, integrity, and availability: a*

Canadian perspective," Studies in Health Technology and Informatics, vol. 29, pp. 286-298, 1996.

[7]. Katsikas S. K. and Gritzalis D., "*Information systems security: facing the information society of the 21st century"*. Chapman and Hall, 1996.

[8]. Fernández-Alemán L. L., Señor I. C., Lozoya P. A. O. and Toval A., *"Security and privacy in electronic health records: A systematic literature review"* Journal of Biomedical Informatics Elsevier Inc. 46:541–562, 2013.

[9]. Westin A. F., *"Privacy and freedom"*. New York: Atheneum; 1967.

[10].Dusserre L., Ducrot H. and Allaërt F. A., "*L'information médicale, l'ordinateur et la loi"*. Editions médicales internationales, 1999.

[11].Allaert F. A., Dusserre L. and Leclercq L., *"The Security of Medical and Hospital Information Systems"*. Springer-Verlag France, Paris, 1997.

[12].Studies and Statistics on IT Claims in France," *National survey carried out for the CLUSIF by GMV Council*, 2001.

[13].Centers for Medicare & Medicaid Services *"Electronic Health Records [Definition]"*, 2016. Accessed on 31st January, 2020. Reterive from https://www.cms.gov/ ehealthrecords/..

[14].Chenthara S., Khandakar A. Wang H. and Whittaker F. *"Security and Privavcy-Preserving Challenges of e-Health Solutions in Cloud Computing"*. IEEEAccess, 7: 74361-74382, 2019.

[15].Harris T., *"Cloud computing - An overview"*, Whitepaper, Torry Harris Business Solutions, 2010.

[16].Huth A. and Cebula J., "*The basics of cloud computing"*, Carnegie Mellon University, Produced for US-CERT, 2011.

[17].Yu S., Wang C., Ren K. and Lou W., *"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing"*. In: 2010 Proceedings IEEE, INFOCOM, San Diego, CA, USA, pp. 1–9, 2010.

[18].Li M., Yu S., Ren K. and Lou W., *"Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multiowner Settings"*. In: International Conference on Security and Privacy in Communication Systems, Singapore, Singapore, pp. 89–106, 2010.

[19].Garcia-Morchon O. and Wehrle K., *"Efficient and context-aware access control for pervasive medical sensor networks*". In: 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, pp. 322–327, 2010.

[20].Zhu L., Zhang C., Xu C., Liu X. and Huang C., *"An efficient and privacy preserving biometric identification scheme in cloud computing",* IEEE Access, 6: 19025-19033, 2018.

[21].Li W., Xue K., Xue Y. and Hong J., *"TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage"*, IEEE Trans. Parallel Distributed System., 27(5):1484-1496, 2016.

[22].Xue K., Xue Y., Hong J., Li W., Yue H., Wei D. S. and Hong P., *"RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage"*, IEEE Trans. Inf. Forensics Security, 12(4):953-967, 2017.

[23].Wei J., Liu W. and Hu X., *"Secure data sharing in cloud computing using revocable-storage identity-based encryption"*, IEEE Trans. Cloud Computing, 6(4):1136-1148, 2016.

[24].Amini S., Verhoeven R., Lukkien J. and Chen S., *"Toward a security model for a body sensor platform".* In: 2011 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 143–144, 2011.

[25].Cui H., Deng R. H. and Li Y., "*Attribute-based cloud storage with secure provenance over encrypted data"*, Future Generation. Comput. Syst., 79(2):461-472, 2018.

[26].Lee W. B. and Lee C. D., *"A cryptographic key management solution for HIPAA privacy/security regulations"*, IEEE Trans. Inf. Technol. Biomed.,12(1):34-41, 2008

[27].Guo L., Zhang C., Sun J. and Fang Y., *"PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks"*. In: 2012 32nd IEEE International Conference on Distributed Computing Systems, Macau, China, pp. 224–233, 2012.

[28].Kumar M., Fathima M. and Mahendran M., *"Personal health data storage protection on cloud using MA-ABE"*. International Journal of Computer Applications, 75(8):11–6, 2013.

[29].Chi P. W. and Lei C. L., *"Audit-free cloud storage via deniable attribute-based encryption*", IEEE Trans. Cloud Computing, 6(2):414-427, 2018.

[30].Li W., Liu B. M., Liu D., Liu R. P., Wang P., Luo S. and Ni W., *"Unified fine-grained access control for personal health records in cloud computing"*, IEEE Journal Biomed. Health Informatics, 23(3):1278-1289, 2018.

[31].Zhang C., Zhu L., Xu C. and Lu R., *"PPDP: An efficient and privacy preserving disease prediction scheme in cloud-based e-healthcare system",* Future Generation Computer System", 79:16-25, 2018.

[32].Zhu H., Huang R., Liu X. and Li H., *"SPEMR: A new secure personal electronic medical record scheme with privilege separation"*. In: 2014 IEEE International Conference on

Communications Workshops (ICC), Sydney, NSW, Australia, pp. 700–705, 2014.

[33].Sunagar V. and Biradar C., *"Securing public health records in cloud computing patient centric and fine grained data access control in multi owner settings"*. International Journal Science and Applied Information Technology, 3(4):18–21, 2014.

[34].Bahtiyar S. and Çaglayan M., "*Trust assessment of security for e-health systems"*. Electron. Commer. Res. Appl., pp 164–177, 2014.

[35].Shrestha N. M., Alsadoon A., Prasad P. W.C., Hourany L., and Elchouemi A*., "Enhanced e-health framework for security and privacy in healthcare system"*. In proceedings of Sixth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, pp.75-79, 2016.

[36].Kim S., Sung M. and Chung Y., *" A framework to preserve the privacy of electronic health data streams*". Journal of Biomed Inf, pp 95–106, 2014.

[37].Chen Y. Y., Lu J. C. and Jan J. K., *"A secure EHR system based on hybrid clouds"*, Journal of Medical Systems., 36(5): 3375-3384, 2012.

[38].Karakıs R., Güler I., Çapraz I. and Bilir E., *"A novel fuzzy logic-based image steganography method to ensure medical data security*. Comput Biol Med, pp 172–183, 2015.

[39] Kester Q., Nana L., Pascu A., Gire S., Eghan J., and Quaynor N., "*A Security Technique for Authentication and Security of Medical Images in Health Information Systems".* In: 2015 15th International Conference on Computational Science and Its Applications, Banff, AB, Canada, pp. 8–13, 2015.

[40].Simplicio M., Iwaya L., Barros B., Carvalho T. and Naslund M. *"SecourHealth: a delay tolerant security framework for mobile health data collection"*. IEEE J Biomed Health Inform, 19(2):761–72, 2015.

[41].Kahani N., Elgazzar K., and Cordy K., *"Authentication and Access Control in e-Health Systems in the Cloud"*. In: IEEE International Conference on High Performance and Smart Computing (HPSC), Big Data Security on Cloud (Big Data Security), New York, NY, USA, pp. 13–23, 2016.

[42].Gajanayake R., Iannella R. and Sahama T., *"Privacy oriented access control for electronic health records"*. e-Journal of Health Informatics 8(2):175–86, 2014.

[43].Rezaeibagha F., and Mu Y., *"Distributed clinical data sharing via dynamic access control policy transformation"*. International Journal of Medical Inf., 25–31, 2016.

[44].Sahi A., Lai D. and Li Y., "*Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan"*. Computer in Biology and Medicine, Elsevier, 78:1–8, 2016.

[45].Chen T. S., Liu C. H., Chen T. L., Chen C. S. Bau J. G. and Lin T. C., *"Secure dynamic access control scheme of PHR in cloud computing",* Journal of medical Systems, 36(6): 4005- 4020, 2012.

[46].Pecarina J., Pu S., and Liu J. C., *"SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds*". In proceedings of 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, IEEE, pp. 99-106, 2012.

[47].Chinnasamy P. and Deepalakshmi P., *"Design of Secure Storage for Health-care Cloud using Hybrid Cryptography"*. In proceedings of Second International Conference on Inventive Communication and Computational Technologies (ICICCT), IEEE, pp. 1717-1720, 2018.

[48].Omotosho A., Adegbola O., Mikail O. O. and Emuoyibofarhe J., *"A secure electronic prescription system using steganography with encryption key implementation"*. arXiv preprintarXiv:1502.01264, 2015.

[49].Li M., Yu S., Zheng Y., Ren, K.. and Lou W., *"Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption"*. IEEE transactions on parallel and distributed systems 24(1): 131-143, 2012.

[50].Sharma M., Bai Y., Chung S. and Dai L, ".*Using risk in access control for cloud-assisted e-health*". In proceedings of 14th International Conference on High Performance Computing and Communications and 9th International Conference on Embedded Software and Systems, IEEE, pp.1047-1052, 2012.

[51].Sakr A., Yaacoub E., Noura H., Al-Husseini M., Abualsaud K., Khattab T. and Guizani M., *"A secure client-side framework for protecting the privacy of health data stored on the cloud*. In proceedings of Middle East and North Africa Communications Conference (MENACOMM), IEEE, pp. 1-6, 2018.

[52].Sharma S., and Balasubramanian V., *"A biometric based authentication and encryption framework for sensor health data in cloud"*. In Proceedings of the 6th International Conference on Information Technology and Multimedia, IEEE, pp. 49-54, 2014.

[53].Patra D., Ray S., Mukhopadhyay J., Majumdar B., and Majumdar A. K., *"Achieving e-health care in a distributed EHR system"*. In proceedings of 11th International Conference on e-Health Networking, Applications and Services (Healthcom 2009*)* (IEEE), pp. 101-107, 2009.

[54].Azeez N. A. and Van der Vyver C. (2019), "*Security and privacy issues in e-health cloud-based system: A comprehensive content analysis"*. Egyptian Informatics Journal, Elsevier, 20(2):97-108, 2019.

[55].Albarki I., Rasslan M., Bahaa-Eldin A. M., and Sobh M., "*Robust Hybrid-Security Protocol for HealthCare Systems"*. Procedia Computer Science, 160: 843-848, 2019.

[56].Okediran O. O., "*A security scheme for patient information Privacy in digital medical imaging"* University of Pitesti Scientific Bulletin: Electr. & Computers Science, 19(2):13-24, 2019.

[57].Okediran O. O., *"A hybrid cryptosystem and watermarking for secure medical image transmission"* Asian Journal of Research in Computer Science, 5(1): 1-14, 2020.

[58].Han H., Huang M., Zhang Y. and Bhatti U.A., "An *architecture of secure health information storage system based on blockchain technology".* In proceedings of International Conference on Cloud Computing and Security, Springer, Cham, pp. 578-588, 2018.

[59].Cao S., Zhang G., Liu P., Zhang X., and Neri F., "*Cloud-assisted secure e-Health system for tamper-proofing EHR via blockchain"*. Information Sciences, 485: 427-440, 2019.

[60].Zaghloul E., Li T. and Ren J., "*Security and Privacy of Electronic Health Records: Decentralized and Hierarchical Data Sharing using Smart Contracts"*, International Conference on Computing, Networking and Communications (ICNC): Cloud Computing and Big Data, 2019.