Exploring Access to EHR by Emergency Patients Using Multimodal Biometrics

I.A Ogbodo

Department of Computer Science, University of Nigeria Nsukka, Nigeria

***Abstract*--- Handling emergency situations in healthcare industry usually require immediate and sudden attention. Despite the emergency nature of such conditions, some vital information from the patient's previous health history is needed prior to the commencement of treatment or care. Delay in accessing the electronic health record (EHR) of emergency patients could result to catastrophic and damaging effects. The use of approaches such as token, smart card, hospital number etc., in order to access and secure the patient's health records has proven ineffective in emergency situations since the patient could be unconscious. Moreover, those traditional means of authentication maybe lost, forged, forgotten or stolen. Again, the drawbacks associated with unimodal biometric access control for EHR such as spoof attacks, noise etc. reduces the effectiveness of systems developed with the single biometric mode. The aim of the paper is to examine comprehensively the use of biometrics approach, in particular, the multimodal biometrics for: (1) accessing quickly the appropriate section of the EHR of emergency patients, (2) identifying patients accurately and (3) providing security and privacy of the confidential patient. The review revealed that multimodal biometrics often majorly and practically fused at the matching score level seems to be a better option of securing and improving easy access to emergency patient's digital health records, and ensures privacy and security of EHR. The implication of the research was that researchers wishing to develop biometric systems for EHR should consider using appropriate multimodal biometrics while adopting means of securing the biometric templates so as to improve efficiency and performance.**

***Keywords*--- Biometrics, Multimodal biometrics, Health emergencies, EHR, EHR Access.**

I. INTRODUCTION

Over the years, the need to keep records of a patient's health history such as drug prescriptions, laboratory tests, vital signs, diagnoses etc., to assist health personnel in delivering effective health care, cannot be overemphasized. With the advent of information technology in health industry, most hospitals in developed countries and some hospitals in developing countries now adopt the electronic health record (EHR) to facilitate quick and inexpensive healthcare delivery. An EHR is the digital form of the conventional paper health record of a patient that is generated, updated and maintained over time by healthcare providers in a healthcare delivery setting in order to provide improved quality healthcare and continuity of care[1]. It also ensures the accessibility and availability of a patient's health record for the administration of healthcare.

Making the health record of a patient available before the commencement of care is very important as it ensures that the patient is treated based on his/her peculiarity and previous health records. The use of EHR is even more crucial in emergency situations. This is because they are the cases that need fast and immediate attention for the retrieval of some relevant records or details of a patient to avoid treating the patient in error and also to render the best care that suits the patient.

Accessing the EHR of a patient by health personnel without restriction to the level of information even in emergency situations may lead to breach or violation of a patient's privacy[2]. There should be a limit to the information of a patient exposed to healthcare professionals that administer care to ensure security. This is due to the nature of risks associated with that kind of record especially if it gets to the hands of people with ulterior motives[3]. A patient with HIV status for instance, may be stigmatized and deprived from benefitting from certain things such as job if there is violation of such confidential health data of the patient or if there is unwise decision to grant health personnel complete access rights to a patient's health record.

Biometric technology in healthcare has proven to be extremely beneficial in various ways by uniquely and easily identifying a patient, enabling faster access to EHR especially for emergency patients (their fundamental data), preventing medical identity theft, allowing for the maintenance of privacy and confidentiality of a patient's EHR, etc. Biometric technology includes the use of fingerprints, iris, face, voice, palm veins, etc to provide a one-to-one relationship between a patient and his/her EHR[4]. Its benefits supersedes that of the non-biometric approaches that involves the use of smart cards, wearables, passwords, PINs etc. to provide access, identification, security and privacy of the health records.

In this paper, we explored some unimodal and multimodal biometric solutions provided by various researches to provide the necessary privacy, security and confidentiality of a patient's EHR and for ensuring that the fundamental health records of an emergency patient are easily accessible to health professionals in a pre-hospital care setting.

II. THE DEMANDS OF EMERGENCY CASES IN HEALTHCARE

Recently, the health sector has witnessed enhanced care delivery to patients through the use of the EHR in the way that it enabled quick, fast and timely access to patient's health records anytime and anywhere[5]. The very many benefits of EHR in healthcare cannot be overemphasized. According to [1] the bedrock of every effective and efficient health record system is the correct and unique identification of the patients. When patients are accurately identified and their health records quickly accessed while preserving patient's privacy and confidentiality, it makes the EHR system effective, accepted and suitable for use in cases of emergency. Emergency situations in healthcare are unforeseen occurrences that require that sudden attention of care be provided to the patient in danger immediately. Assessing the EHR quickly before commencing care of an emergency patient so as not to treat the patient in error is very important in emergency situations.

Moreover, emergency conditions normally occasions that the processes involved in accessing the EHR be changed to address the peculiarity of such situations[6]. The uniqueness of the emergency department makes it demanding and complex to access the EHR of emergency patients which is why any technique that allows for easy access of the categorized emergency health record must be adopted[7]. There is the consciousness of time and mindful access to the health information when rendering care to emergency patients[8].

III. PRIVACY, CONFIDENTIAL, AND SECURITY ISSUES IN EHR ACCESS

The advancement in technology in the health industry opened the door to issues concerning the privacy and confidentiality of the patient's health records. Also, the move by healthcare organizations to go electronic and operate the health records of patients electronically has raised issues of privacy and confidentiality of these records especially when care is received from different healthcare providers. There is need for the privacy of patients to be preserved because those administering the care to the patients may also know them and when sensitive information are disclosed by the healthcare personnel, it may lead to devastating effects on the patients such as lack of trust, resistance to convey important and necessary information when needed, hiding, stigmatization and committing of suicide by some patients.

Privacy of EHR of a patient, according to [9] is the right of that patient which guarantees that his/her health records are not disclosed to the general public and that only authorized persons could gain access to it. A patient's privacy could only be violated by an authorized health personnel where the health records of that patient are accessed and used in the way that the patient does not want[10]. This is why there should be control to the level of health information of patients disclosed to the authorized health personnel.

Moreover, patient confidentiality is the right of a patient that ensures the privacy of the health data[6]. The confidentiality of a patient must be considered first in anything done in healthcare [11], even when innovations are made in the sector. This could foster healthy relationships between the patients and health professionals. The HIPAA (Health Insurance Portability and Accountability Act) mostly adopted by many EHR systems is the legislative law that protects the EHR of patients and ensures that every health organization secures their patient's confidential health data [6][11]. The dictates of the law must be observed when accessing the EHR of patients before or during administration of care [5] even in emergency settings. The recorded cases of violations of privacy and confidentiality of patient's health records and the methods of storing the EHR made patients even more aware in the issues of privacy as this could lead to lack of trust of the system and reduced healthcare delivery since patients would not be free to disclose confidential or sensitive information [7]. Patients now prefer that certain of their health records be made available to certain health practitioners[12]. In other words, the health records should be categorized such that the psychiatric doctor for instance, accesses only the part of the EHR that will improve the patient's mental well-being.

These major challenges of privacy and confidentiality must be tackled in order to instill and build trust in the lives of patients that entrust their sensitive health data in the hands of healthcare organizations to offer better security measures.

A major concern for the adoption and acceptance of the EHR is the security of the patient's electronic version of the health records. The method of ensuring security of the EHR is of great concern to the patient since any breach of security normally affects them. Securing the health data is very paramount in health industry. Security is the protection of the health records from unauthorized access. The primary goals of security in healthcare are: confidentiality- it entails ensuring that only those authorized to have access to the health data can actually gain access to it, integrity- it entails ensuring that the health data is correct and not altered by unauthorized means or persons, availability- it entails making the health data accessible when needed by an authorized health personnel[6][13]. These are also the security requirements of every EHR system. Electronic health needs to address these identified security requirements so as to guarantee security of the EHR system[14]. Confidentiality could be ensured by adhering strictly to the HIPAA act, while for ensuring integrity, audit log could kept whenever the EHR is accessed especially in emergency cases. The security method to use in EHR systems moreover, depends on the following[15]: user-friendliness, cost effectiveness, availability, confidentiality, integrity, accountability and the capacity to work both in shared healthcare settings and locally.

It is pertinent to note that the numerous advantages offered by EHR could truly be realized if the privacy, confidentiality, security and integrity concerns are handled[12]. A systematic review of the security and privacy solutions offered by many EHR systems was carried out in [6] and it discovered that in making sure that the security and privacy of patients are guaranteed, efforts should be made to adopt the rules in the regulations of the EHR data. It revealed further, that most of these systems use the HIPAA standards and regulations to ensure confidentiality of the EHR. Also, it considered the health records as one of the most confidential information contained in the personal data of a person.

Moreover, a review of the issues involving the security, privacy and accountability of the EHR of patients was presented in [16]. It maintained that for the patients to completely accept or trust their health data in the EHR systems, that the trio- privacy, security and accountability must be ensured. Privacy could be ensured by a method that retrieves to authorized persons seeking for access into the EHR system only the portion that he/she is permitted to, and making both the patient and health physicians to be in charge of the EHR system. In other words, privileges should be given to the users of the system. Security could be ensured through the use of cryptography. Finally, those that accessed the EHR systems should be held accountable for the actions that they carry out in the system. In as much as the work recommends that cryptography be used for security, it is not the only way as would be observed in this research.

IV. APPROACHES FOR ACCESSING THE EHR

There are various approaches for accessing the EHR and ensuring control over unauthorized use or violation of privacy and security. These approaches could be non-biometric or biometric in nature. We first examined some non-biometric approaches for accessing the EHR before exploring the biometric techniques.

A. Non-biometric Approaches/Technologies

Using Non-biometric approaches are the traditional methods adopted to ensure that the EHR are accessed only by authorized health personnel and that patients are identified or authenticated correctly[5][11]. They are broadly categorized into two: Possession-based and Knowledge-based non-biometric methods. The possession-based non-biometric method in healthcare is the use of what one owns such as wearable technologies, smartcards, USB, etc. to ascertain the identity of a patient and consequently access the EHR of that patient[16]. Generally, these possession-based technologies could be lost, stolen, damaged, destroyed, forged, etc. making it hard to access the EHR and leading to lack of trust. Researches in [17], [18] and [19] demonstrated the use of the possession-based technology in healthcare. The knowledge-based non-biometric approach however, involves the use of what one knows such as PINs, passwords, and tokens (both soft and hard) etc., to ensure accurate identification, authentication and provide access to the EHR[20]. These knowledge-based methods could be copied, hacked, forgotten, guessed, shared, revealed, etc. In [21] and [22], the use of knowledge-based non-biometric approach was developed.

B. Biometrics Approach and Biometrics System

Biometrics are those distinguishable biological traits that identifies or verifies a person to be unique from every other person through the use of either physiological characteristics such as fingerprints, iris, face, palm print, etc. or behavioral characteristics such as keystroke, voice, gestures, etc. In healthcare, it is ascertaining and proving who a patient really is using the biological attributes of that patient such as facial features, fingerprints, voice, iris, etc. It is found out to be the best approach so far out of so many other approaches for accurate and automatic patient identification and security of health data from unauthorized access[20][23]. According to [24], biometric systems are those computer systems that works by capturing from a person the unique biometric data, preprocesses the captured data in order to extract the required features, then matches this data with the set of stored template in the database so as to make a decision of either to reject or accept the data based on the matching score. Biometric systems could moreover, be seen as a pattern matching system or technique that attempts to match the collected unique pattern with a template already stored in the database. This technique is the basis for differentiating a person uniquely using the behavioral or physiological features[25]. Every biometric system has two fundamental methods which are Authentication and Identification methods[26]. The former involves checking the biometric feature of a person captured from the scanner with a particular template stored in the database in a one-to-one fashion to ascertain whether the person is actually who he says he is while the latter involves checking the captured biometric feature against many other biometrics features in the database in a one-to-many fashion to find out who a person is. There is a preference for the use of biometrics for patient identification when compared to the non-biometric methods because the biometric technology is non-invasive[5]. Moreover, authentication using biometrics has become a widely adopted means of verification in almost all sectors and industries because of the convenience and security it offered. Verification is the same authentication. [24] observed that identity of an individual could be proved through either verification which entails checking the assertion of a claimant who is to be identified in order to decide whether to accept or reject his claim based on the result of the check or identification which gets someone recognized from a database without him claiming to be someone. These two terms are mostly used interchangeably in health biometric systems for patient recognition. Additionally, the issues that influenced the adoption of the biometric systems were emphasized in

[27] as: financial issues-concerns the financial feasibility of the biometric; operational issues-concerns activities especially at the enrollment, authentication and storage stages; system issues-these include downtime, disasters, cyber attacks; human issues-entails privacy issues and the trust on the part of the patients, and physiological characteristics possessed by patients-concerns the possibility of some patients not possessing the particular physiological or behavioral characteristics.

The appropriateness of the biometric features used in biometric authentication[26] depends on $C^2U^2P^2A$: Collectability-concerns the ability of getting biometric features without difficulty, Circumvention-concerns how easy it is to impersonate or copy the biometric feature with a replacement, Uniqueness-concerns the ability of the biometric feature collected to be unlike any other person's biometric feature for easy separation, Universality-the ability of the biometric feature to be generally possessed by all, Permanence-This concerns the measure of how long the biometric feature remains constant in a person without varying, Performance-concerns the technology used to capture the biometric feature, whether it is fast, robust, and above all accurate, Acceptability-concerns how people receive or accept the biometric technology without having issues when their unique traits are captured and their data accessed. It is important to note that the performance of the biometric technique used is very important to the EHR system. Three major factors that affect the performance of any biometric system are highlighted in [28] as accuracy, speed and storage. The accuracy of the biometric system is very crucial since the systems may accept a wrong person as the right person (false match) or reject a right person (false non-match) out of error. How high or low the errors are, gives an insight as to determine which biometric to use in the EHR system for ensuring security and privacy of the sensitive health data. Also, how fast the biometric system identifies an individual is important. Some biometric systems require the overall identification process to be executed in seconds while for others time is not a factor. Moreover, while storing the biometric template in the database, the compression technique adopted to do so affect the storage size. The storage size in turn influences how fast the biometric template is retrieved during authentication/verification. Equally, the overall infrastructural cost of maintaining the biometric data is affected.

V. USE OF BIOMETRICS IN HEALTHCARE FOR EHR ACCESS

With the wide adoption of EHR systems by many healthcare organizations, breaches of security by health workers, medical identity theft occurrences, and the legal regulation protecting patient's privacy, a new form of identification/authentication such as biometrics is a necessity [29]. A survey carried out in [24] reports that biometrics such as fingerprint, face, iris hand geometry, palm print, voice, and signature are already widely applied in various fields while some others such as earlobe, knuckle brain/EEG, heart sound/ECG are still at their research phase and not used widely in different areas. Health sector is not an exception in this technological advancement. Since the health records of patients are constantly being accessed in order to provide enhanced healthcare, there is need to adopt a better form of authentication that enables accurate and timely identification, and ensures security instead of using the non-biometric methods that has lots of disadvantages [29]. Biometrics is used mainly in healthcare for authentication, access control, encrypting health data, identifying patients and health personnel in order to have remote to the health records, and verifying the identity of a patient[15]. Using biometrics in healthcare has several advantages over other traditional security methods. Some of the advantages are: unfailing and simple user authentication, limited or controlled access rights to the health data; cost maintenance reduction, accurate identification for remote access to the health data, security and accessibility of the EHR, health information encryption[15], discouragement of medical identity theft, accurate accountability of user operations, user-friendliness and faster verification[30]. Surveys carried out in [13] and [15] established that the use of biometric in electronic health proved to reliably offer improved security benefits than the conventional authentication approaches because of the numerous advantages that biometric authentication provides. In as much as biometrics was predominantly used for user authentication to achieve security in healthcare, it was equally used for health data encryption. The challenge of managing and storing the key in cryptographic-based systems is a major concern. It was highlighted in [16] that bio-cryptography was applied in healthcare to enhance the management of cryptographic keys. The biometric templates of the keys are equally encrypted using the traditional cryptographic approach. Additionally, in an overview of the biometric techniques presented by [27], fingerprint recognition biometric was discovered to have been in use for a long time and is still currently in use, while iris scanning biometric technique was considered to be more reliable than other biometric solutions.

A. Unimodal Biometric Systems for EHR Access, Identification and Authentication

Unimodal biometric systems are systems designed to use only a single biometric technique to provide authentication, identification, access control, security and privacy of an individual. The single mode biometric traits used could be physiological or behavioral. Some researches that utilized unimodal biometric systems in healthcare were examined:

A self-service patient kiosk that used palm-vein biometrics of the Fujitsu Palm Secure in order to address the issues associated with identifying patients accurately, patient verification and medical identity theft was proposed in [4]. The system has the ability to secure the EHR of patients, ensure privacy of patients, authenticate patients, simplify

registration process, enhance check-ins, update and improve healthcare delivery. The palm-vein biometric was chosen because its failure to enroll rate is nearly zero, implying that it is easy for any patient to use the biometric by scanning the veins of the palm. Also, it is hygienic to use since the scanning process is contactless. Moreover, the palm-vein is difficult to spoof because it leaves no prints or traces on the scanner. A fingerprint unimodal biometric technique that utilized an if-only-if relation to provide remote access to a patient's EHR to any requesting health personnel if and only if the fingerprint of the patient captured during emergency matches the biometric template stored in the database was developed in [2]. The system utilized a token-free approach to access the EHR of emergency patients while preserving patients' privacy policy. Mobile technology was used to send the captured fingerprint of emergency patients to a central server to be authenticated and provide access to the needed EHR so as to render accurate and improved healthcare delivery. Again, the security of the delicate health records of patients together with that of the biometric template that generates the cryptographic access key for accessing the encrypted health record was guaranteed in a cancelable finger-vein bio-cryptographic system embedded in a smartcard in [31]. One of the system's major and commendable contributions was the use of cancelable biometric approach to take into consideration the security of the biometric template used to access the cryptographic key that unlocks the sensitive health information of patients. This is very crucial because the biometrics features does not change and once the pattern gets into the wrong hands, it becomes a serious threat to the security of that person. For prevention of leakage of health information during the EHR access, the system was embedded in a smartcard which holds both the biometric template and the encrypted delicate health information. Finger-vein biometrics was utilized to offer authentication to the template that binds the cryptographic access key.

B. Multimodal Biometric Systems for EHR Access, Identification and Authentication

Multimodal biometric systems are pattern recognition systems that combine two or more of physiological or behavioral traits of an individual in order to provide security and privacy of a person. In healthcare, more than one biometrics could be used to verify a patient or health personnel, restrict access to the EHR data of patients, identify patients and secure the health data. The use of biometrics for identification, verification or security has inbuilt benefits but unimodal biometrics presents challenges of accuracy, enrollment rate, vulnerability to spoofing attacks, noise in the sensed data, non-universality, etc[25]. Also, these challenges are mainly noticed in face recognition while fingerprint recognition is mostly vulnerable to spoofing attacks. A biometric system is termed multimodal even if the relationship between the modalities used is an "OR" relationship. Moreover, the goal of every biometric system is to reduce any of these rates: false accept rate (FAR), false reject rate (FRR) and failure to enroll rate (FTE). A survey[24] highlights that the challenges inherent in unimodal biometrics systems makes multimodal biometrics to serve as a better solution for offering enhanced accuracy. Multimodal biometric features combines and joins data at different levels such as sensor, feature extraction, matching score, and decision levels in order to enhance the overall performance and strength of the whole system in a process known as multimodal biometric fusion[24], [25] . Moreover, most multimodal biometrics mainly implement this fusion at the matching score levels because of the availability of information that the level functions with, the simplicity and the ease with which those biometric traits could be combined. Two phases in biometric fusion of multimodal traits were identified in [32] as (1) the choice of suitable biometric traits to fuse and (2) the design of the best biometric fusion method which could be carried out at any of the already established levels. The research further highlights two modes of multimodal biometrics to be (1) biometric enrollment mode and (2) biometric verification mode. The enrollment mode involves capturing and preprocessing the biometric traits in order to extract the features and store. The verification mode involves checking whether there is a match between the already enrolled feature and the real-time captured biometric traits. Finally, from the same research, it was observed that multimodal biometric verification systems are of three kinds: multi-algorithm (use of various algorithms to verify one biometric characteristic), multi-biometric systems (use of more than one different modes of biometric characteristics) and hybrid systems (use of the combination of multi-algorithm and multi-biometric systems). Multi-biometric are normally termed multimodal biometrics by most researches.

C. Applications of Multimodal Biometrics in Healthcare

Biometric technology was applied in [32] into embedded systems such as mobile phones, PDAs mainly for identifying users of such devices. A system that assigned security levels based on the sensitivity and criticality of the softwares hosted in the web servers and accessed through WLAN using multimodal biometrics as an additional authentication method in order to provide security to the hosted web applications and shield it from web hackers was proposed in [33]. A user that needs access to the web applications must connect through the advanced authentication server which adds extra security using the biometric features and is charge of the enrollment and authentication. Four levels of authentication were proposed for offering authentication to web applications based on their importance. Level 2 authentication utilizes unimodal biometric to offer authentication giving the system the ability to be viewed as both unimodal and multimodal systems. A biometric system was proposed by [29] after a survey with focus on the use of biometrics for patient authentication of the EHR system and for ensuring security, used fingerprint, face and iris to identify the patient and access the health information of that patient in an emergency setting (heart

attack). In [33], a semi-continuous biometric framework that combined both physiological (face) and behavioral (keystroke) traits fused at the matching score level to provide secured authentication when the health records of patients are accessed after it has been monitored and stored in the cloud was developed. The fusion of keystroke and face recognition multimodal biometric traits was used for authentication mainly because they were both effective and the use of the individual biometric traits may not offer the needed increase in performance. The use of semi-continuous authentication system equally ensured the security of the system which entails verifying a user constantly for the whole period of using the system, not just at the beginning of the session. This though, may make the entire use of the system tiring and boring to the user. A multimodal biometric that fused two biometric systems which are face recognition and iris scanning in order to offer access control, patient privacy and security to the EHR was implemented in [35]. Both biometric traits were fused because of the need for: verification accuracy, improved system performance, reducing the failure to enroll rate and increasing the population of the users handled. It implemented biometric fusion at the matching score level and observed that iris scanning has a higher performance than face recognition system when tested individually but the general performance of the system improved with the fusion of the two traits. Also, the multimodal biometrics deployed in a tablet PC and consisting of the fusion of voice and signature was used as a means of authentication to secure the EHR and restrict access to it[36]. The use of the multimodal biometrics was to achieve greater accuracy and eliminate the challenges present in unimodal biometric systems. Biometric fusion of the traits was at the matching score level. The two biometric traits were chosen because they are non-intrusive and resemble the normal scenario of patient authentication. The work in [37] developed a multimodal biometric system that is fused with cryptographic algorithm at the matching score level called biometric cryptosystems. The preprocessing of the biometric traits was done in order to extract the required features which are encrypted with the hyper image-encryption algorithm and the template is stored in the database. Moreover, [38] developed a multimodal biometric system that fused four finger biometric traits (fingerprint, finger-shape, finger-vein and finger-knuckle) to provide authentication. The fusion was carried out the matching score level because of the ease and high performance of doing it at that level. Finally, a multimodal biometric system that fused iris scanning and fingerprint traits which are used for easily and reliably accessing the EHR of patients in an emergency setting and equally provide security was developed by [3]. The level of health information revealed to the health personnel that access the EHR is restricted by categorizing the health information into confidential, basic and emergency attributes in order to preserve the privacy and confidentiality of patients. During emergency such when the patient is unconscious, the biometrics traits of the patient is used to provide access to that patient's EHR where as the health personnel access only the emergency section of the EHR after successful biometric authentication. The system observed that fingerprint biometric performs better than the iris scanner in terms of response when the biometric traits are tested individually.

VI. DISCUSSION

After a careful research, it was observed that privacy, security, patient data integrity and confidentiality are the major issues mainly affecting the full adoption and user acceptance of the EHR. Almost all the EHR systems adopted the HIPAA legal regulation and standard to protect the privacy of patients. The non-biometric traditional methods such as password, wearables, etc., have issues of security and equally the tendency of being lost, stolen, forgotten, hacked, and revealed. Biometrics has a wide application in healthcare industry and was generally accepted as a better option of limiting access to the EHR and providing security/privacy of the health data of patients. Its application in healthcare ranges from being used for accurate and prompt identification of patients, verification/authentication purposes, ensuring security and privacy of the health data, and as a mechanism for access control. Biometrics was mainly used for identification and verification of patients before their health records are accessed. Also, earlier biometric systems and even present ones mostly used the fingerprint biometric technique because of its simplicity, ease of use and cost effectiveness of its scanner, although, recent biometric systems now adopt other biometric techniques such as iris, palm-vein, etc.

Again, many of the researches agreed that the use of only a single mode biometric system (unimodal) hinders the overall goal of achieving security of the EHR because of the problems inherent in the unimodal biometric systems such as noisy sensors, susceptibility to spoofing attacks, user acceptance issues, etc.

Moreover, there was a general acceptance that the use of multimodal biometric systems is the solution to the challenges of the single-mode biometric system in healthcare. Also it was observed that fusion of multimodal traits was practically and predominantly carried out at the matching score level because the level has data available to operate with.

VII. CONCLUSION

In conclusion, multimodal biometrics provides better system performance than the unimodal biometrics. However, when multimodal biometrics are being fused, efforts should be made to choose the best fusion approach while putting into consideration the various kinds of biometric traits because the overall system performance is increased when some biometric traits are fused with some particular matching kinds of biometric traits. Again, more work needs to be done in ensuring that the captured biometric traits are themselves well protected because the revelation of one's permanent biometric

trait could pose a serious threat to the patient. Finally, as pointed out by [22], no matter the advanced technique used to secure and limit access to the EHR of patients, it must be easily made available and accessible.

REFERENCES

[1] WHO, "Electronic Health Records: Manual for Developing Countries," *WHO Libr. Cat. Publ. Data, West. Pacific Reg.*, pp. 1–78, 2006.

[2] J. R. Díaz-Palacios, V. J. Romo-Aledo, and A. H. Chinaei, "Biometric access control for e-health records in pre-hospital care," *Proc. Jt. EDBT/ICDT 2013 Work. - EDBT '13*, p. 169, 2013.

[3] A. Omotosho, O. Adegbola, B. Adelakin, A. Adelakun, and J. Emuoyibofarhe, "Exploiting Multimodal Biometrics in E-Privacy Scheme for Electronic Health Records," *J. Biol. Agric. Healthc.*, vol. 4, no. 18, pp. 22–33, 2014.

[4] J. Napua, "Growth of biometric technology in self-service situations," *Fujitsu Sci. Tech. J.*, vol. 47, no. 1, pp. 68–74, 2011.

[5] A. A. Khwaji, "EHRs at King Fahad Specialist Hospital : An overview of professionals ' perspectives on the use of biometric patient identification for privacy and confidentiality , taking into consideration culture and religion," Massey University Albany, Auckland New Zealand, 2016.

[6] J. L. Fernández-alemán, I. C. Señor, P. Ángel, O. Lozoya, and A. Toval, "Security and privacy in electronic health records : A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2015.

[7] O. Ben-assuli, "Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments," *Health Policy (New. York).*, 2014.

[8] A. Sarcevic, "Electronic Health Records in Emergency Medical Care," pp. 1–4.

[9] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *Int. J. Med. Inform.*, vol. 80, no. 2, pp. e26–e31, 2011.

[10] J. Bleiberg and N. Yaraghi, "Balancing privacy and security with health records." The Brookings Institution, 2015.

[11] T. Seymour, D. Frantsvog, and T. Graeber, "Electronic Health Records (EHR)," *Am. J. Heal. Sci.*, vol. 3, no. June, 2012.

[12] A. Shenoy and J. M. Appel, "Safeguarding Confidentiality in Electronic Health Records," *Cambridge Q. Healthc. Ethics*, vol. 26, pp. 337–341, 2017.

[13] [E. Okoh and A. I. Awad, "Biometrics Applications in e-Health Security : A Preliminary Survey," vol. 2, no. May 2015, pp. 92–104, 2015.

[14] E. Okoh, "Biometrics Solutions in e-Health Security A Comprehensive Literature Review Biometrics Solutions in e-Health Security - A," Luleå University of Technology, 2015.

[15] A. Enrique, F. Zuniga, and K. T. Win, "Biometrics for Electronic Health Records," pp. 975–983, 2010.

[16] A. Omotosho and J. Emuoyibofarhe, "A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records," *Int. J. Appl. Inf. Syst.*, vol. 7, no. 8, pp. 11–18, 2014.

[17] I. K. Al-azwani and H. A. Aziz, "Integration of Wearable Technologies into Patients ' Electronic Medical Records," *Qual. Prim. Care*, vol. 24, no. 4, pp. 151–155, 2016.

[18] A. Darwish and A. E. Hassanien, "Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring," *Sensors*, vol. 11, pp. 5561–5595, 2011.

[19] F. L. Maloney and A. Wright, "USB-based Personal Health Records: An analysis of features and functionality," *Int. J. Med. Inform.*, vol. 79, no. 2, pp. 97–111, 2010.

[20] L. Wang and C. A. Alexander, "Medical Applications and Healthcare Based on Cloud Computing," *Int. J. Cloud Comput. Serv. Sci.*, vol. 2, no. 4, pp. 217–225, 2014.

[21] F. W. Dillema and S. Lupetti, "Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment," in *HealthNet*, 2007.

[22] J. Künzi, P. Koster, and M. Petkovic, "Emergency Access to Protected Health Records," *Med. Informatics a United Heal. Eur.*, pp. 705–709, 2009.

[23] L. Wang and C. A. Alexander, "Applications of Automated Identification Technology in EHR / EMR," *Int. J. Public Heal. Sci. e*, vol. 2, no. 3, pp. 109–122, 2013.

[24] A. H. Mir, S. Rubab, and Z. A. Jhat, "Biometrics Verification : a Literature Survey," *J. Comput. ICT Res.*, vol. 5, no. 2, pp. 67–80, 2011.

[25] S. Patil, "Biometric Recognition Using Unimodal and Multimodal Features," pp. 6824–6829, 2014.

[26] G. Patni and S. Sharma, "Biometric System Introduction with its various Identification Techniques," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 3, pp. 866–871, 2017.

[27] A. Chandra and R. Durand, "The uses and potential of biometrics in health care Are consumers and providers ready for it?," *Int. J. Pharm. Healthc. Mark.*, vol. 2, no. 1, pp. 22–34, 2008.

[28] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Commun. ACM*, vol. 43, no. 2, pp. 90–98, 2000.

[29] S. Manimekalai, "A Study on Biometric for Single Sign on Health Care Security System," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 6, pp. 79–87, 2014.

[30] A. Iacona, "Health Care Information Technology : Securing the Electronic Health Record with Biometric Technology Health Care Information Technology : Securing the Electronic Health," *Rev. A J. Undergrad. Student Res.*, vol. 15, pp. 4–8, 2014.

[31] W. Yang *et al.*, "Securing Mobile Healthcare Data : A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem," *IEEE Access*, vol. 6, pp. 36939–36947, 2018.

[32] J. Wang, Y. Li, Y. Zhang, and Y. Huang, "Implementing Multimodal Biometric Solutions in Embedded Systems," in *Biometrics - Unique and Diverse Applications in Nature, Science, and Technology*, no. May 2014, 2008.

[33] S. Kumar, S. Paul, and D. K. Shaw, "Design and Modeling of Real Time Multimodal Biometric Authentication System," *J. Comput. Sci.*, 2017.

[34] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "Bio-Authentication for Layered Remote Health Monitor Framework.," *J. Med. Informatics Technol.*, vol. 23, 2014.

[35] S. J. Al-hijaili and M. Abdulaziz, "Biometric in Healthcare Security System , Face - Iris Fusion System Biometrics In Health Care Security System , Iris-Face Fusion System," *Int. J. Acad. Res.*, vol. 3, no. January 2011, 2011.

[36] S. Krawczyk and A. k. Jain, "Securing Electronic Medical Records Using Biometric Authentication," *Secur. Manag.*, pp. 446–452, 2005.

[37] D. Jagadiswary and D. Saraswady, "Multimodal Biometric Fusion Using Image Encryption Algorithm," *ACM*, 2016.

[38] J. Peng, A. A. A. El-latif, Q. Li, and X. Niu, "Optik Multimodal biometric authentication based on score level fusion of finger biometrics," *Opt. - Int. J. Light Electron Opt.*, vol. 125, no. 23, pp. 6891–6897, 2014.