ISSN No:-2456-2165

ECG-Based Biometric Schemes for Healthcare: A Systematic Review

Emmanuel Nannim Ramson[1]*, Musa Nehemiah[2], John Chaka[3]
[1]Department of General Studies Education, Federal College of Education, Pankshin, Jos, Plateau State, Nigeria
[2]Department of Mathematical Sciences, Abubakar Tafawa Balewa University, Bauchi, Nigeria
[3]Department of Computer Sciences, Federal College of Education, Pankshin, Jos, Plateau State, Nigeria

*Corresponding Author: Emmanuel Nannim Ramson

Abstracts:- The use of Electro Cardio Gram (ECG) signals as a biometric modality has been well-established in healthcare applications and facilities because of its robustness against security attacks compare to the traditional biometrics (e.g. Iris, facial, fingerprint biometrics etc.), which provide momentary verification and require direct contact or proximity. However, recent biometrics based on physiological signals such as ECG, photoplethysmogram, Arterial Blood Pressure etc. possess continuous, aliveness and internal nature properties which make them suitable and unique for providing security and privacy in healthcare remote monitoring systems. The emergence of Internet of Medical Things (IoMTs), biosensors and Wireless Body Area Networks (WBANs) devices have enabled easy monitoring of our vital signals for diagnosis and made remote health monitoring more convenient and seamless. These innovations however, brought with them other challenges including various security threats to communicated or stored data which require stringent security measures to protect the sensitive personal patients' data. To the best of the authors' knowledge, previous surveys provide limited discussion on ECG-based biometric security and privacy solutions for healthcare institutions, especially in health remote monitoring systems. In order to provide broader discussion on this regard, this review systematically presents the various ECG-based biometric techniques/measures designed to provide security and privacy of patients' data in healthcare institutions. Taxonomy of ECG-based biometric techniques for healthcare security is presented. Discussions, challenges and research opportunities were presented to guide healthcare institutions, especially in developing countries to embrace ECG biometric technology in order to mitigate the glaring dangers of security threats on patient's health records.

Keywords:- *Biometric; Electrocardiogram; Healthcare; Security; Remote Monitoring Systems.*

I. INTRODUCTION

The emergence of Internet-of-Things (IoTs), cloud computing [1-3] and Wireless Body Area networks (WBANs) [4, 5] birth a new dimension of Doctor-Patient relationship and enhance continuous monitoring of patients in remote mode [2]. Different terms have been referred to this process such as Telemedicine or Telehealth[6-9] or electronic health (e-health) [2, 10, 11] or remote patient monitoring [12, 13]. This process brought great improvements from the conventional ways of patients visiting healthcare institutions for one diagnosis or the other. Nowadays, different healthcare applications have been embedded in consumer devices to remotely collect physiological information of a patient and provide automatic treatment [14] This is particularly important for monitoring patients with critical diseases that require continuous monitoring, follow-ups of disease treatment, health assessment and prediction, for instance, people living in rural areas and senior citizens. More so, it helps in situations where visiting hospitals or a medical centres is restricted due to disease pandemic such as in the case during Corana Virus (COVID-19) pandemic [3, 15, 16]. In this case, remote monitoring of patients becomes imperative to ensure continuous monitoring of patients [3, 6, 17]. Remote patient monitoring systems are often used in conjunction with Wireless Sensor Networks (WSNs), Body Sensor Networks (BSNs) and various IoTs devices to monitor discharged patients from the ICU and patients with special needs [2]. Wireless Body Area Networks (WBAN) or Wireless Body Sensor Networks (WBSN) constitutes of nano-sensors and actuators that collects data from patients for the purpose of monitoring. These sensors are place in the body, on the body or on patients' cloths to capture patients' data and transmit it over a wireless network to the server [18]. WBSN has been emerged as the center of mobile physical condition monitoring, which intends to convalesce the severe scarcity of accessible medical resources [19].

The proliferations of Internet of Medical Things (IoMTs) devices such as low-cost sensors or Implantable and Wearable Medical Devices (IWMDs) that monitor our vital signals and daily activities have made remote health monitoring more convenient and seamless[20, 21]. IoMTs is the most emerging era of the IoTs, which is a collection of various smart medical devices connected within the network through the internet [21, 22]. In IoT-cloud-based e-Health systems, underlying IoTs networks enable communication between users, services and servers, with medical data stored in the cloud [2]. The IoT-based healthcare system uses connected bio-sensors that collects various biomedical signals and connectivity to share/communicate the signals received instantaneously to the internet and health care providers[23]. The reliability, security, and accuracy of these sensors and wireless devices has a direct effect on the timely access to information for patient under monitoring. More so, family members can be tempted to share these wearable devices in many application scenarios. For instance, an elderly couple is more willing to share a biosensor for health

ISSN No:-2456-2165

monitoring in order to reduce cost. Therefore, personal identification becomes expedient in order to avert erroneous diagnosis of patients[24]. Erroneous identification of patients by medical practitioners is considered one of the leading cause of medical errors which render serious risk on the patient safety [24, 25]. The confidentiality of medical data is important, not only to protect the health of the patient, but also to protect their privacy [26].

Different monitoring systems have been developed to monitor vital parameter of the human body. The monitoring systems use bio-signal sensors to capture and communicate the significant sign parameters of heart beat, blood pressure and body temperature etc. [10, 11, 27]. These bio-signals do not only carry personal data for the health patient but also carry unique features that can uniquely identify such patient and can be used to secure the patient data [28]. More to secure communications and data storage in system security, it also include rigorous identity authentication and authority management of data access [29].

These cluster of innovations such as IoMTs, IWMDs, biosensors, WBANs and numerous lightweight communication protocols used for remote patients monitoring systems brought with them other challenges including various security threats to communicated or stored information which require stringent security measures to preserve the integrity, confidentiality and privacy of patients' data in heath institutions. There are different techniques developed such as cryptography, biometrics, watermarking, and blockchain-based security for health data security [30]. This study aims at presenting the various electrocardiograms (ECG)-based biometric techniques designed to provide security and privacy of patients' data in healthcare institutions. Previous related reviews of ECG biometric systems have been investigated given the evidences from the literature [2, 14, 30, 31]. A study by [2] presented an overview of privacy and security issues in IoT-cloud-based e-Health systems and performed a comparative analysis of major privacy and security issues, solutions and architectures used in IoT-cloud-based e-Health systems. Hathaliya et al. [31] performed a review and analysis of state-of-the-art proposals to maintain security and privacy in Healthcare 4.0. The review discussed blockchain-based solution to give insights to both researchers and practitioners communities. A study by [30], present a comprehensive survey on state-of-the-art techniques such as cryptography, biometrics, watermarking, and blockchain-based security for health data security. The authors also discussed the contribution of reviewed techniques in terms of their objective, methodology, type of medical data, important features, and limitations. Another survey presented by [14] explored various security and privacy threats to healthcare systems and discussed the consequences of these threats. The authors also discussed existing security measures proposed for healthcare systems and discussed their limitations. These surveys, however, lack in broad discussion of ECG-based biometric security and privacy solutions for remote health monitoring systems. More so, the studies did not employ systematic review methodology to report their study. The main contributions of our study are as follows;

- We conduct systematic literature review of the various ECG-based biometric schemes proposed to mitigate security and privacy issues in healthcare institutions.
- We provide taxonomy of security and privacy measures/solutions achieved using ECG-based biometric schemes from the reviewed papers.
- Discussions on open challenges, limitations and future directions were presented to guide future researchers.

The subsequent sections of this study are organized as follows: Section 2 discusses the security and privacy concerns in healthcare institutions. Section 3 presents the review method adopted in this study. Section 4 presents the results. Discussions, challenges and research opportunities are presented in sections 5; finally section 6 concludes the study.

II. SECURITY AND PRIVACY CONCERNS IN HEALTHCARE INSTITUTIONS

The security and privacy of individual's data is non-negotiable in every data-driven institution, especially in healthcare institutions. The security of digital systems especially in healthcare applications is even more critical as it comprise the sensitive data of patients. Security of patients' personal record and access to health information systems has continued to be a cause of concern for both patients and health institutions. According to Newaz et al.[14] modern technologies such as IoTs, IWMDs, biosensors, and BANs have certainly enhanced overall healthcare systems for patients and medical professionals. However, the use of these technologies introduced more complexity in software and hardware which would require stringent security and privacy strategies to mitigate the impact of attacks in healthcare systems [14, 31]. IoTs authentication techniques face various security threats, common among them include device impersonation attack, injection attack, side-channel attack, eavesdropping and interference, sleep deprivation attack, DDoS attack, Replay attack and man in the middle attack [32]. Hospitals and medical centers are vulnerable to Hackers due to their basic need for regular electronic records, care directives, medicine information and therapeutic records, in order to provide the necessary care for the patient. In the healthcare environments, patient reports are very sensitive and need to be secured to prevent attacks [33].

Authentication of individual is the basic required factor for patient data privacy and identity verification [34]. Methods to authenticate individual fall either based on what you know (*knowledge based*), such as the use of password or based on what you have (*token based*), such as the use of smart card or based on what you are (*biometric*), such as the use of fingerprint [35]. Knowledge based and token based authentication have been ineffective and inefficient to ensure the security and privacy of individual data with so many security risks including forgetfulness, loss, and theft [36-40]. Authentication based on what you are also called "biometric" emerged to cope with the vulnerabilities of the previous methods [41-43]. Biometric system is the measurement of the unique physiological or behavioural characteristics of an individual. It either identifies or authenticates an individual based on the unique features [44, 45]. While identification

ISSN No:-2456-2165

process involves revealing the unknown subject using the supplied data into the model, authentication process however, accepts or rejects claims of known subject by analyzing the supplied data into the model [46]. In the aspect of security, ECG is considered to be a *medical biometric* because it's an important physiological signal with much medical value [7]

A. Electrocardiogram as a Biometric Modality

The biometric system is grouped into physiological characteristics and behavioural characteristics such as fingerprint[47], iris [48], hand veins [49] and keystroke dynamics [50], signature [51], respectively. The use of biometric has proven to be more effective in security as compared to the traditional measures (knowledge based and token based methods), because biometric require the use of biological feature of the user before authentication and granting of access. Nevertheless, researchers have demonstrated the possibility of spoofing attacks on traditional biometric systems [52-54]. Traditional biometrics also known as external or hard biometrics, such as fingerprint, iris, facial, signature, keystroke dynamics etc. are more prone to spoofing attacks compared to the internal or hidden biometrics[55, 56]. Researchers have therefore explored the use of hidden biometrics such as vein, DNA and brain pattern to identify individuals based on features hidden in the body parts of human subjects[57-59]. ECG signal is considered a hidden biometrics which is based on the unique features of physiological signal produced by the electrical heart variability.

ECG (also known as EKG) is a commonly used biomedical signal, characterized by a high degree of intervariability [60]. The ECG signals provide information that can aid to understand and analyze cardiac activity of a person's heart rate, rhythm and morphology [61-63]. The ECG tool is non-invasive that provides measurement of electrical signals generated from the heartbeat activity. ECG is the process of recording of the depolarised electrical activity of the heart muscles. The depolarization is propagated as a wave across the entire body including the heart. The current produced as a result of this wave is unique and relies on the structure of heart and body. A device called electrode are placed on human skin have been used to collect ECG recordings. These electrodes detect changes in the electrical activity on the skin caused by depolarizing pattern of the heart muscles during each heartbeat. This produced a waveform known as ECG waveform which comprises of five waves called PQRST waves (see Fig. 1) [7, 64]. These waves give information about the electrical activities of the heart; and they have been used for diagnosis of various heart disorders [65-67]. ECG is one of the most used physiological signals that can be detected non-invasively, and has become a must-have signals due to its ease-of-monitoring, ease-of-detection, individual uniqueness and rich in clinical value[68]. ECG for Biometric systems was first introduced in 1977 by the US military [69]. The ECG features were found to be unique to individual and applicable as a biometric trait for human identification [70-72], and it falls under human physiological characteristics [73].

Based on the features required for recognition, ECG authentication systems are classified into two; fiducial and non-fiducial. The fiducial methods extract six characteristic points from the heartbeat wave (P, Q, R, S, T, U), these are the onset and the offset of the heart beat waves. Also, these are used to extract some features such as amplitude difference between consecutive fiducial points and latency. On the other hand, non-fiducial techniques analyze the entire ECG wave or isolated heart beats to extract features statistically based on the overall morphology of the waveform [7, 74]. Some methods utilized hybrid of fiducial and non-fiducail features as features into their models in order to improve the authentication stability. Characteristics such as inimitability, suitability, accessibility and comfortability make ECG highly promising for healthcare systems compared to traditional biometrics [75]. ECG-based biometric have the advantage of achieving two important diagnoses of patients at the same time. While using the ECG signals for identification, the diagnosis of the patient's cardiovascular diseases can also be obtained [76].

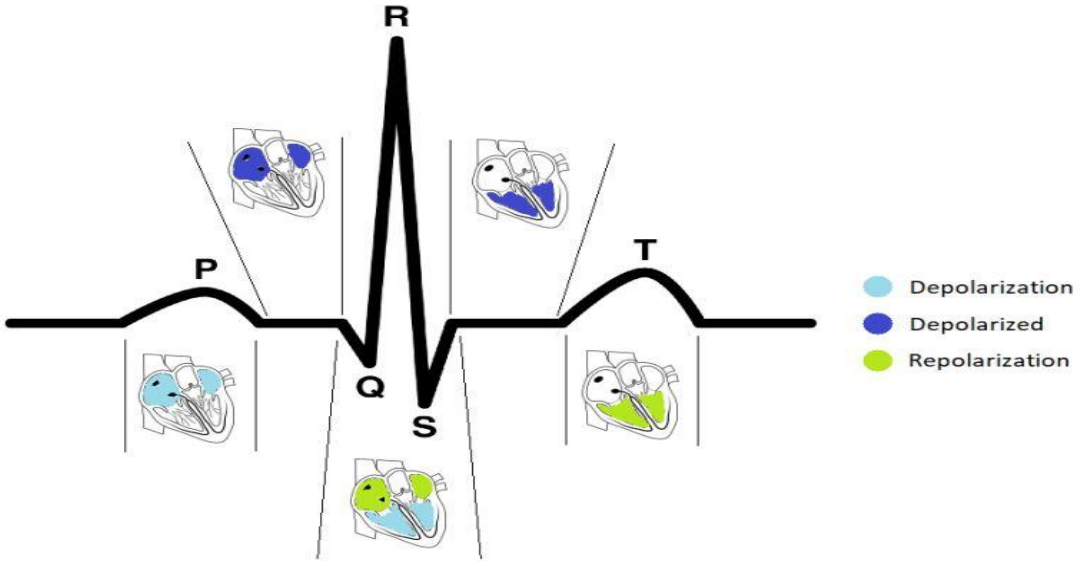

Fig. 1: The ECG wave depolarization and repolarization sequence[44]

The applications of ECG as a medical biosignals have been investigated for various tasks in different domains of applications such as healthcare, driving and security[77, 78]. ECG is not only a gold standard cardiac signal, but also unique to each individual [79]. ECG-based biometric systems have drawn the attention of researchers in the last decades, which are based on using the human heartbeat variability from ECG to identify and authenticate individuals. ECG biometric is considered more difficult to be compromised by spoofing attacks than the existing biological traits [45, 80]. In addition, ECG signals unlike the external biometrics, certifies that the subject is real and alive [81, 82]. ECG is the most successful biometric with aliveness feature that has been used for various applications especially in healthcare facilities [83]. Over the years, several ECG based security and privacy measures to conceal data and/or authenticate patients against a third party and to provide access for only authorized individuals have been developed and investigated [14, 30, 31].

III. METHOD

This study uses a systematic Literature Review (SLR) which is repeatable and can be validated. Literature reviews should be valid, reliable, and repeatable [84]. This review adopted the SLR verified guidelines by Evidence-based Software Engineering project proposed for carrying out evidence-based reviews[85, 86]. There are basically three stages that are required for SLR which include planning the review, conducting the review and reporting the review. In order to reduce the possibility of researchers' bias, the following research protocol were used to guide the selection and analysis of review papers; (I) the research questions; (II) the search strategy; (III) study selection criteria and (IV) the data extraction and synthesis of results.

A. Research Questions (RQ):

This review focus on presenting different strategies and solutions proposed using ECG-based biometric to secure, preserve and protect patients' data in healthcare systems. Based on this premise, the following research questions were formulated to guide the study;

- ***RQ1:*** *What are the ECG-based biometric schemes designed to provide security and privacy of patients' data in healthcare institutions?*
- ***RQ2:*** *What are the security and privacy measures/solutions achieved using ECG signals in the proposed schemes?*

B. Search Strategy:

We searched two electronic databases; IEEE Xplore[1] and PubMed[2] to retrieve primary studies for the review. These databases were selected because they publish original scientific papers from health and computing related journals and conferences. Terms which best describe the type of papers required for the study were used to perform the search in the respective databases. Terms such as "Electrocardiogram", "ECG", "EKG" "Biometric, "Security", "Authentication, "Identification", "health Institutions", "Healthcare" and "Hospitals" were concatenated using OR and AND Boolean operators to form the search string, this is because most databases support Boolean operators [84]. The "OR" operator usually combines synonymous keywords while "AND" operator joins the main terms or group of synonyms in the search string [87]. The search string was modified to suit the specific databases criteria for search strings. The search was bounded to relevant papers published between 2000 to April, 2023 (current date of conducting this research). This year range is considered appropriate because ECG-biometric early research publication can be traced back to 2001[70, 71].

C. Study selection criteria:

In conducting SLR, researchers are advised to set boundaries as to which paper is eligible to be included for the study. These criteria should be practical and state clearly the type of papers to be included or excluded for the study [86]. We selected papers that will best describe or answer the research questions formulated in the study. For a primary paper to be included for the study, it must have the following, otherwise, it is excluded; it must show the evidence of the application of ECG-based biometric for the purpose of providing security and privacy of patients' data in healthcare facilities. The study must be evidence based and passed through peer-reviewed process published in either journals, conferences or workshops. Also, the paper must be reported in English Language. The most updated and complete duplicate papers were included. Reviews, Books, Encyclopedia, Posters, book chapters, keynotes, and editorials were excluded for the study. The tittles and abstracts of the searched papers were examined by the researchers in light of the stated inclusion criteria before inclusion of the papers.

In order to provide final check on inclusion/exclusion, full text assessment was conducted by reading through the manuscripts from abstract to conclusion in order to ascertain the quality of the paper [84].

D. Data extraction and synthesis:

Relevant data required answering the research questions and for the purposes of meta-analysis were extracted from the included papers, taking note of the papers that do not report any of the meta-data required for the study. These data were used to answer the research questions.

Figure 2 shows the processes involved in selecting of papers for inclusion for the study. The process begins with the selection phase, when literatures are searched through the electronic databases, forward and backward searching [84]. In this study, two popular databases for medical and computing related published papers were searched using the search string formed. IEEE Xplore Library populated 67 published papers while PubMed database returned 59 published papers, making a total of n=126 papers. The second phase involves screening the papers returned by the search performed on the databases, which was done in light of the inclusion criteria stipulated in this study. 71 papers were screened out due to reasons such as they are literature review papers, book chapters or books, commentaries, magazines,

[1] https://ieeexplore.ieee.org/Xplore/home.jsp

[2] https://pubmed.ncbi.nlm.nih.gov/?otool=uiclib

ISSN No:-2456-2165

title of research not relevant for the study and duplicate paper. 55 papers were tested for eligibility for inclusion. Here, full-text reading of the screened papers was performed to assess the quality of the papers, 17 papers were excluded for reasons such as ECG signal as a biometric was not discussed, paper discussed ECG signal out of the context of healthcare and full-text was missing. 38 papers were included for the study. However, backward search was performed and 7 papers were discovered and added with the included papers making 45 papers which were included and reviewed in the study.

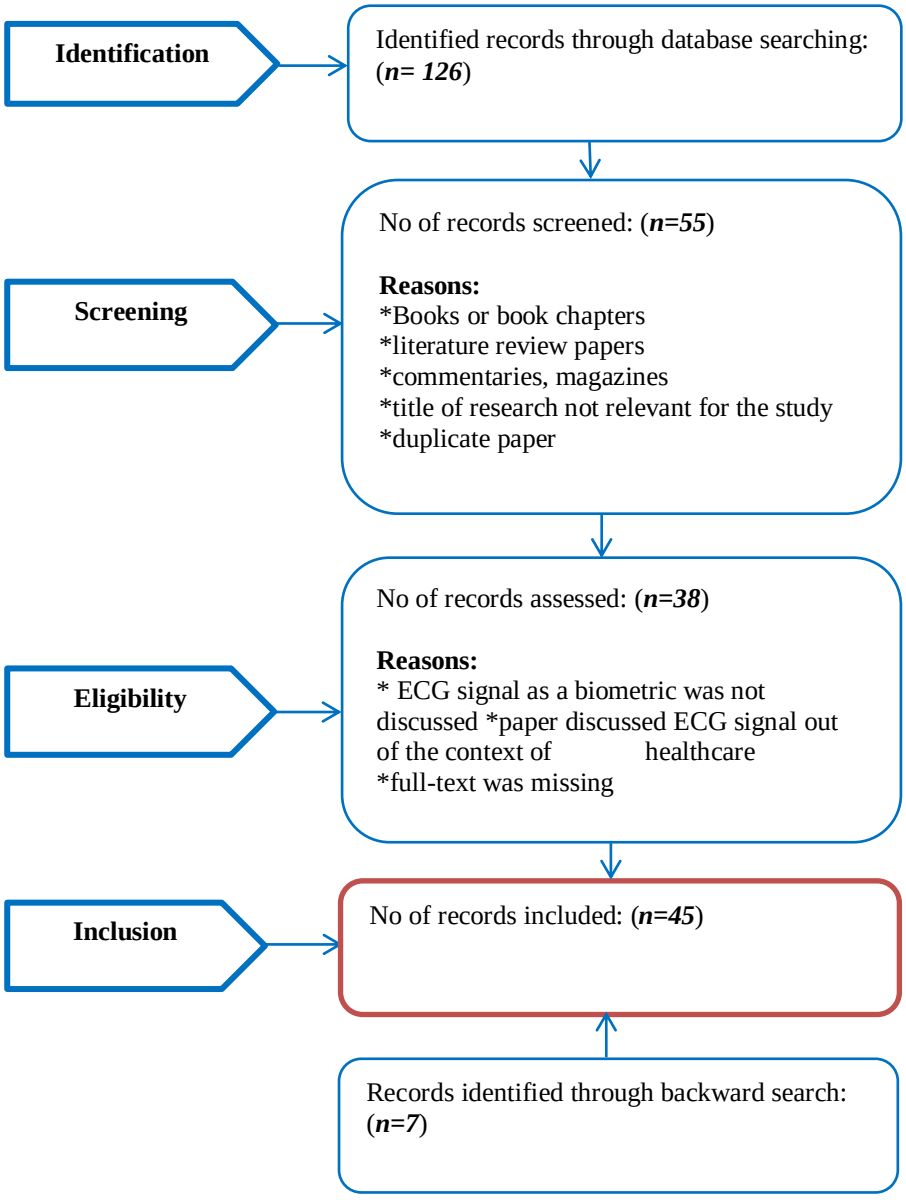

Fig. 2: Paper selection processes

IV. RESULTS

This section reports the various security and privacy techniques proposed for healthcare applications in the included papers.

A. *ECG biometric and IoT-based e-healthcare systems*

Biometric systems either identifies or authenticates an individual based on the unique features of the individuals behavioral or physiological traits [44, 45]. The process of biometric identification or authentication is usually divided into two; enrolment and identification/authentication (see fig. 3). During enrolment process, the individual behavioural or physiological biometric features that uniquely identify the enroller are extracted and are kept in the features database (cloud). During this process, preprocessing can be applied on the raw features to remove artifacts, noises etc. in order to improve the quality of the extracted features. The second stage (identification/authentication) involves validating the claims of users accessing the system. While identification process involves revealing the unknown subject using the supplied data into the model, authentication process however, accepts or rejects claims of known subject by analyzing the supplied data into the model. Fig 3 shows a high-level architecture of biometric verification system using mobile ECG. Here, the ECG signal is collected from an individual by a mobile device and is transmitted to the biometric verification system in a remote center over wireless networks [88]. There are different ECG-based approaches toward achieving security in healthcare that have been proposed to

ISSN No:-2456-2165

secure patients data and to verify/identify individuals before giving access to health services and/or devices. ECG based biometric is among the biometrics that does not require extra hardware to be used in health care systems and can be mainly used in IoT based health care systems where data is transferred on internet [89]. IoT basically refers to a network of smart devices connected ubiquitously and are deployed to perform tasks such as health monitoring, environmental sensing, and smart city applications. The healthcare IoT refers to IoT with special interest on medical applications[90]. There are different ECG-based biometric systems proposed in the literature to identify and authenticate patients [7, 40, 64, 75, 76, 79, 88, 89, 91-104].

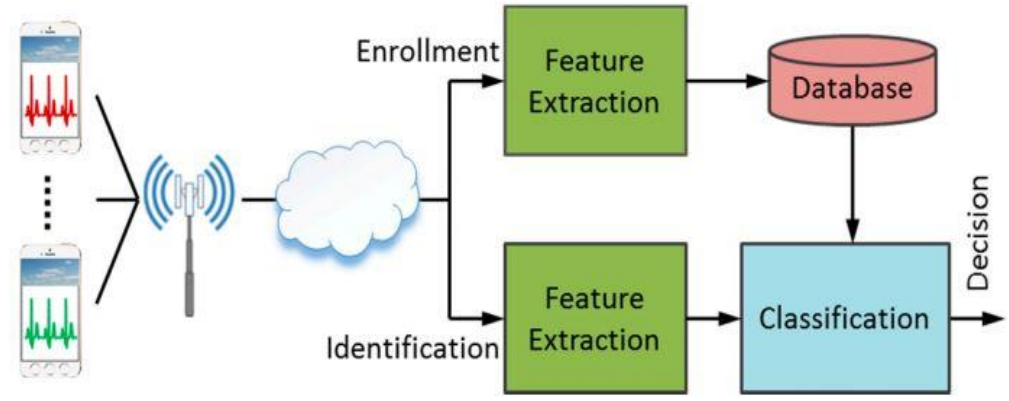

Fig. 3: Patient authentication process using mobile ECG [88].

In remote patient monitoring, it is imperative the data is coming from the right patient. Previous methods such as the use of password credentials and one-time authentication using traditional biometrics are not well-suited for continuous authentication and monitoring of patient at real time. Fig. 4 shows IoT-based patient monitoring system structure [105]. Researchers in [91], proposed a probabilistic activity-aware ECG-based patient authentication scheme (KNN+Bayesian) for the purpose of remote health monitoring of patients in hospitals. Perturbation of the ECG signal due to physical activity is a major obstacle in applying the technology in real-world situations. The proposed method explored the impact of activity on the performance of the ECG based biometric system unlike previous methods. Although the proposed method achieved verification accuracy of 88%, the dataset captured from only 17 person was small and only from normal healthy subjects. A study by [92] proposed a framework for continuous identity verification based on ECG signals for security enhancement in the healthcare information systems context. The proposed framework was evaluated using ECG signal from 32 healthy individuals and achieved EER of 2.75%±0.29. A study by [7]proposed a method that used ECG signal for identity authentication in remote monitoring settings, well-suited for welfare monitoring environments which require remote, efficient, and continuous authentication of the involved parties. The authors addressed the problem of intra-subject variability of the ECG signal due to psychological changes (emotional activities). A solution based on template updating was proposed for welfare monitoring environment. The proposed method was evaluated from ECG signals of 43 volunteers; an EER of 3.96% was achieved, which represents 15% reduction from a particular dataset in the absence of template updating.

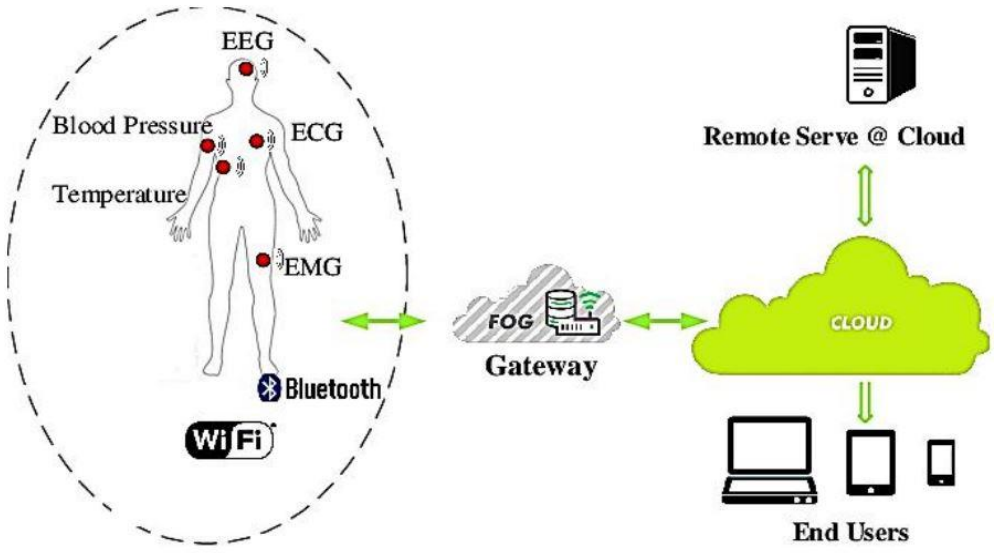

Fig. 4: Health IoT based healthcare monitoring framework [105]

ECG features as well as can be used to authenticate individuals accessing the healthcare services, it can also be used to encrypt patient personal data against various attacks. Huang et al. [93] proposed a scheme for reusable authentication and encryption scheme using ECG signals for e-Health systems. In the proposed scheme, the ECG signals was used to authenticate patients' identities and at the same time encrypt their personal health records, the scheme also enables the reuse and preserve the privacy of the same ECG signal. A study conducted by [96] proposed an ECG biometric scheme to authenticate patients in a healthcare system while concealing the privacy of their transmitted ECG. Linear Prediction Coding (LPC) technique was used to hide the ECG sensitive data, an alternative to the fuzzy vault scheme. LPC technique ensures a similar security level while offering a low computational complexity and communication overhead compared with the fuzzy vault scheme. An acceptable recognition rate was also achieved. A study by [98] proposed ECG-based scheme for IoT-based healthcare capable of authenticating subjects using noisy ECG input while protecting the privacy of stored ECG templates. Unlike most of the existing works that were evaluated on artificially-added noises on real or simulated ECG signals, this proposed scheme was tested on real world noisy ECG signals, taking the advantage of singular vector decomposition and boost the scheme efficiency when applying it to authentication procedure. Evaluation on both online dataset and real world experiments shows that the proposed approach can effectively and efficiently authenticate patients while ensuring the privacy of templates.

In other to mitigate the challenges of acquiring ECG signals from mobile device, authors in [88] proposed a two-stage classifier, combining probabilistic random forest method with the wavelet distance template matching. The proposed system's performance was found better than either of the random forest classifier with ECG fiducial feature extraction and the template matching classifier using wavelet distance measure in terms of low computational load and verification accuracy. A study by [94] proposed a two-phase authentication method using artificial neural network (NN) models, a "General" NN model for preliminary screening, and the "Personal" model for specific recognition. The proposed method was tested on data from 50 subjects and achieved a fast authentication within only 3 seconds and with acceptable recognition performance. A study by [95] presented a study of ECG-based authentication system suitable for security checks and hospital environments. The authors used Amang ECG (amgecg) toolbox within MATLAB to investigate the effect of two factors; ECG slicing time (sliding window) and the sampling time period on identification accuracy. The proposed system achieved a good performance of 92% identification accuracy. However, the optimal slicing and sampling time periods may not remain the same if different datasets are used. A study conducted by [75] proposed parallel ECG based authentication (PEA) for smart healthcare systems based on MapReduce that can effectively search the multimodal ECG feature space of fiducial and non-fiducial features extracted from the ECG signals. The proposed method achieved considerable accuracy and efficiency compared with those of other conventional approaches. CNN based ECG biometric system for authentication in healthcare applications was proposed by [89]. The ECG features extracted from four different databases such as distances between R, P, Q, S and T peaks and were fed into KNN, SVM and CNN models, shows that CNN achieved the best performance using FANTASIA database, with 96.95%.accuracy. A predictive analytic-based ML biometric security mechanism for developing health data security framework for e-healthcare was proposed by [97]. The proposed method is based on multilayer perception model. A secure communication channel is used to make the signal unaffected against interference. The proposed method is applicable to authenticate users. A study by [99] proposed an attention based hierarchical long short-term memory (LSTM) model to learn the biometric representation corresponding to a person. The LSTM learn the temporal variation of the ECG signal in different abstractions while the attention mechanism learns to capture the ECG complexes unique to individual for verification and identification. The proposed model was evaluated with on-the-person and off-the-person ECG datasets and achieved better performance compared to existing methods. Behrouzi et al. [100] developed an authentication application by using ECG signals in Siamese networks (CNN) in healthcare systems. The proposed Siamese networks tackled the problem of imbalanced data, insufficient data for training and the need for retraining when new data is added to the model. The proposed method was achieved a good authentication accuracy of 92% and 95%, respectively. A recent study [64], proposed a method for personal authentication using deep learning models (CNN and LSTM). Features (QRS peaks) from raw ECG signals were extracted and fed into the proposed models. The proposed systems achieved overall accuracy of 98.34% for CNN and 99.69% for LSTM using the PTB database.

ECG-based biometric depends on the ECG signals or waveform to extract unique and salient features that can uniquely identify a subject. However, ECG signals are often affected by different diseases which may affect the normal rhyme of the waveforms, thereby make it difficult to extract these salient features for recognition purposes. There are studies that have investigated the degree of effect of some of these cardiac diseases on the identification of patients in healthcare institutions. A study conducted by [101] proposed a method based on Multilayer Perceptron (MLP) classifier to identify a Cardiac Autonomic Neuropathy Patients (CAN) using Cardioid Based Graph for ECG Biometric. The dataset used were gotten from participants with diabetes from the Charles Sturt Diabetes Complication Screening Initiative (DiScRi). The method achieved classification accuracies of 99.6% for patients with early CAN, 99.1% for patients with severe/definite CAN and 99.3% for all the CAN patients.

A study by [68] proposed a method to improve identification accuracy using dynamic threshold setting to extract the most stable ECG waveform as the template and for test waveforms. The piecewise linear representation (PLR) was used on the ECG signal segment to reduce the data size while maintaining important information of the ECG signal segment. Then dynamic time wrapping (DTW) was used as the identification method. The half total error rate of the ECG biometric system of the proposed method was

ISSN No:-2456-2165

reduced from 3.35% to 1.45%, a significant improvement. Another study by [106] proposed an ECG-based biometric to identify individuals in healthcare systems. This proposed method instead of using fiducial features, features were extracted using Hadamard Transform to get the compressed version of the original signals and were fed into K-NN classifier. The proposed system showed that these compressed ECG signals are robust and effective to unequivocally identify individuals. A study by [107] proposed a two-stage cascaded classification system using wavelet analysis coupled with probabilistic random forest machine learning by utilizing both fiducial and non-fiducial ECG features. The proposed algorithm aimed at improving the accuracy and robustness of human biometric identification using ECG from mobile devices. A study by [102] proposed a wavelet domain multiresolution CNN approach (MCNN) for ECG biometric identification in smart health applications. The proposed method blindly selects a physiological signal segment for identification purpose thereby avoiding fiducial characteristics extraction process. The proposed method when evaluated achieved an average identification rate of 93.5%. A phase-domain deep patient-ECG image learning framework for zero-effort smart health user identification is investigated by [79]. The proposed method applied time-to-phase domain transformation which allow for randomly picking of any ECG segment that has unknown phase (start and end timing) and unknown number of heartbeats, by hiding the phase difference and heartbeat number difference both in a phase loop trajectory. Thereby transforming the ECG signal into an ECG image which was fed into CNN for classification without going through the stress of manual or feature engineering and provide zero-effort ECG-enhanced smart health security. A study by [103] conducted a comparative performance analysis of ECG signal based human identification for both healthy and unhealthy subjects. self-built database with ECG records over a one-month time span from 68 subjects is used for the stability performance of ECG based human identification, where 38 subjects were elderly people with cardiovascular diseases and the remaining subjects are young and healthy subjects. They system performance favours the healthy subjects with 98.14% as against unhealthy subjects with accuracy rate at 95.62%. Jyotishi (2020) proposed two LSTM based architectures for multilead data fusion. Spatial variation of ECG signal was used to enhance the identification accuracy. The proposed approach was evaluated on PTB and MIT-BIH arrhythmia database and achieved identification accuracies of 98.77% and 99.29%, respectively. In a study presented by [104] an ECG-based biometric recognition scheme that can potentially strengthen the security of IoT-based patient monitoring systems was proposed. The proposed method used “subspace oversampling,” technique to create distinct and irreversible templates for a registered patient to avoid the cross-matching problem and privacy invasion. The identity of unknown subjects were determined using only their beat bundles with the help of “subspace matching,” without any additional information required for template construction. The proposed scheme was evaluated using the PTB dataset and identification rate of 99.02% was obtained. A recent study performed by [76] Proposed an approach for patient identification in healthcare systems using ECG signals. The proposed systems used CNN to process patients’ data from different databases with different health conditions and a database of healthy users in various scenarios. The approached achieved a promising performance of at least accuracy of 97.09% identification accuracy with acceptable FAR and FRR. The authors claimed that their proposed approach brings it closer to real life applications in healthcare systems and facilities because of its performance in different health conditions and under various scenarios. However, there is still room for improvement.

ECG signals has rich information that is used within the healthcare to diagnose different Cardiovascular Diseases (CVDs) and related diseases ranging from coronary artery disease to the risk of a heart attack. The healthcare is cautious of storing and sharing ECG data over privacy concerns because of its individualistic nature which is capable of authenticating individual, especially ECG data. De-identification process involves removing all direct identifiers from patient data so that it can be shared without the risk of divulging identity information[108]. Researchers in [108] claimed to be the first to proposed a method to de-identify ECG signals using a Generative Adversarial Network (GAN)-based framework. The authors combined standard GAN loss, an Ordinary Differential Equations (ODE)-based, and identity-based loss values to train a generator that de-identifies ECG signal, at the same time, preserving ECG signal structure and the target cardio vascular condition information. The proposed method was evaluated using MIT-BIH arrhythmia database and achieved identification accuracy of 58.44%, about 8% to random guess (50%) while providing an arrhythmia detection (Normal and Supraventricular Ectopic Beat) performance of 95.66%, and 2.7% reduction in arrhythmia detection. Table 1 gives the summary of ECG-based biometric schemes for healthcare security solutions.

ISSN No:-2456-2165

Table 1: The summary of ECG-based biometric schemes for security and privacy solutions healthcare

Proposed scheme [Reference]	**Security Measure**	**ECG feature**	**Performance Parameter**	**Limitation/ Future Direction**
ECG based identity verification [92]	Authentication	ECG signals	EER	• Limited dataset was used and data from healthy individuals • Proposed to perform field validation in a real-world scenario, and implementation of a pilot system
Template Updating algorithm[7]	Authentication	P wave, the QRS complex, and T wave	EER	• Only few subjects ECG signals were used and from healthy individuals. • Emotions were induced not from real life sources
CNN[79]	Identification	ECG segment	Accuracy	• To explore more databases, ECG attacks and corresponding security enhancement methodologies. • To improve the transformation methods & deep feature learning topologies
Machine learning-based medical Information security framework[97]	Authentication	RR intervals	No performance analysis.	• No system performance analysis was provided • Need to analyse the applicability of proposed system for healthcare applications.
Random forest classifier[103]	Identification	P-QRS-T complexes	Accuracy	• More ECG signals from different sessions of recordings can improve system's performance. • Mechanism of updating training datasets should be carried out to address the problem of feature varying over time for subjects having cardiovascular diseases
K-NN algorithm + Hadamard Transform [106]	Identification	Compressed ECG	Accuracy. Identification system errors	• The proposed method was only tested on only one database containing only healthy individuals' data. • Hadamard Transform can be compared with other set of transforms
ECG- based authentication in noisy Environments[98]	Authentication	P wave, PR interval, QRS complex, J point, ST segment, and T wave	Efficiency (running time), privacy preservation	• Need to improve system robustness by using more data for real noisy ECG signals
1D-CNN, SVM, KNN[89]	Authentication	Distances between R, P, Q, S and T peaks	Accuracy	• Need for more training dataset • Model can be trained using other deep networks
"General" NN model and Personal" model[94]	Authentication	QRS and QRST complexes	FAR, FRR	• Dataset was captured from only 50 subjects • Authentication accuracy can be improved while maintaining a short acquisition time for authentication.
probabilistic approach + random forest + wavelet distance measure[107]	Identification	P, R, T peaks and Q, S Valleys	Accuracy	• The proposed model assumed that one ECG complex represents one Subject which in reality is not
ECG-based Encryption and Authentication[93]	Authentication and encryption	QRS complex	Authentication time (45ms)	• Further studies is required to explore users' revocability on keys and experiment the effect of illness

PLR-DTW[68]	Identification	Waveform	FAR, FRR Running time, half total error rate	• Limited data from small number of enrollers were used • ECG signals collected at rest and from healthy subjects only. • Further study of relationship between storage space and identification accuracy is required
LSTM[40]	Identification	Beat segment	Accuracy	• To explore ECG data collected from different sessions and different physical conditions
GAN[108]	De-identification	ECG signals	Accuracy	• Only two classes of arrhythmia were targeted for detection. • To explore other generator architectures. • To use advanced verificator modules
Two-stage classifier (probabilistic random forest method with the wavelet distance template matching)[88]	Authentication	P- QRS-T complex	Low computational load, accuracy	• The proposed algorithm can be adapted with dual ECG/fingerprint scanning for applications such as in biosecurity and cybersecurity
PEA[75]	Authentication	PQRST, spectral and morphologi cal features	Accuracy	• Proposed method is susceptible to cardiac diseases
MCNN[102]	Identification	random ECG segments	Identification rate	• Explore data representation methods and neural network topologies. • To identify external stimulation-related ECG patterns
LPC[96]	Authentication	ECG window	FRR, FAR	Further studies to improve system performance by • Studying optimal time for reference template refreshment. • Adding a synchronization block for heart rate variability concealment. • studying the optimal number of attempts
CNN, LSTM[64]	Authentication and identification	QRS segments	Accuracy	• Only a single database was used • To study adaptability of the proposed system under various physiological conditions and cardiac disorders
KNN+Bayesian[91]	Authentication	Feature window with multiple heart beats	Accuracy	• Model can be improved by introducing more activity and sensors into the model. • Implementation of verification locally on the mobile device. • Small dataset was captured and only normal healthy subjects were used
Attention Based Hierarchical LSTM[99]	Verification and Identification	intra-beat variation and interbeat variation and P, QRS, and T complexes	Accuracy, EER	• Model performance can be improved by discarding low quality ECG signals
ECM + CNN[76]	Identification	ECG signals	Accuracy	• System performance may be improved using more data and by exploring other deep learning architectures
Siamese	Authentication	ECG signals	Accuracy	• The model performance can be improved using data from different scenarios

Networks (CNN)[100]				
Machine learning (DT-based regression vs. SVM)[95]	Authentication	ECG slicing and sampling time periods	Accuracy	• Slicing and sampling time periods may differ with different dataset
Subspace oversampling and subspace matching[104]	Identification	ECG beat bundles	Identification rate	• Model performance can be improved with more datasets
MLP classifier[101]	Identification	Features from Cardioid based graph gotten from QRS complexes	Accuracy	• Dataset was only from Cardiac Autonomic Neuropathy patients not suitable for a generalized healthcare systems

B. ECG biometric and Body Area Sensor Networks

The Internet of medical things (IoMT), a sub-filed of Internet of things (IoT) used in healthcare environment has enhanced the quality of human life in enabling continuously monitoring the health data of patients without any laboratory requirements. IoMTs communicate physiological elements such as temperature, blood pressure, Electroencephalgraphy (EEG) signals, ECG signals etc. as inputs acquired through sensor network called Body Sensor Network (BSN) [109]. The important underlying technology for health IoT is the Wireless Sensor Networks (WSNs), most especially the Body Sensor Networks (BSNs) [90]. Wireless BSNs a particular case of Wireless Sensors Networks (WSNs) is a technology equipped with sensors which are embedded in the body or attached on a body which collect the physiological elements and transfer them in real-time over a network in the form of multimedia such as text, audio, image, and video. A WBANs consists of a set of mobile and small size intercommunicating sensors, which are either wearable or can be implanted into the human body for monitoring vital signs [18, 110]. WBSN has gained significant interests as an important infrastructure for the real-time biomedical healthcare system, while the security of the sensitive health information becomes one of the main challenges [111]. This raise the alarm over the security of the networks, how to maintain the confidentiality, privacy and integrity of medical data over these communication networks has been a persistent pursuit that require strong security measures against external attacks. Therefore, the need to encode the information communicated against various attacks such as physical attacks, network cyber-attacks, software attacks and encryption attacks is necessary [112]. ECG as a biometric was found to be robust in handling these attacks because of its continuous nature as against the traditional biometrics.

There are different ECG-based authentication schemes and group key management strategies that have been developed to provide security and privacy over the inherent open wireless communicating characteristics in WBANs communication. ECG-based Biometric authentication designed to improve security of Body Area Sensor Networks (BANs) for health applications have been investigated[12, 19, 28, 109, 111, 113-120]. In cryptosystems, key management schemes are crucial to satisfy the security requirements for the storage and communication of the sensitive health information. A study in [111] proposed an energy-efficient approach that can generate and distribute the cryptographic keys using the ECG biometrics in WBSN. The system works by representing the ECG signal in an ordered set and transform the problem of key agreement into the problem of set reconciliation, so as to decrease the necessary transmission bits of the public information. The proposed approached reduced communication bits for key agreement as well as minimize energy consumption by 20%, which shows promising and practical key distribution scheme for secure communications in WBSN. In another study conducted by [113], an ECG biometric representation scheme was proposed called VitaCode, capable of representing the ECG feature in a set with integer elements, which can be combined with the fuzzy biometric cryptography. The set modality was more suitable for the ECG representation than the binary code modality, it also achieve better accuracy compared to the Euclidean distance and hamming distance. In order to explore the specific signal patterns and stochastic pattern uniqueness of the biometric information, a Gaussian Mixture Model (GMM)-based stochastic authentication scheme was proposed by [114]. The proposed scheme utilized the locally captured ECG-IPI signal to avoid key exchange overhead. The proposed approach used different approach from traditional ones by applying stochastic pattern recognition to ECG signal security. The proposed approach achieved tolerance against sample misalignment and the authentication scheme has a low authentication. In [115], a key agreement scheme that allows neighboring nodes in BANs to share a common key generated by ECG signals for the message authentication using improved Jules Sudan (IJS) algorithm was proposed. The proposed ECG-IJS key agreement scheme could be implemented in a “plug and play” manner, which means reduction in key distribution overheads. The proposed scheme demonstrated better performance to secure data communications over BANs better than the existing methods. The use of re-deployed keys or manual setups to identify sensor nodes that are physically attached to the same human

body in BAN has been cumbersome and error-prone, Peter et al.[116] designed and implemented stages required realizing an ECG-based authentication protocol to identify sensor nodes attached to the same human body. Unlike the previous methods, the authors implemented ECG-based authentication with consideration of practical implications of the low cost sensors and resource-constrained BAN platforms, couple with uncertainties originating from sensors and processing. The authentication protocol ensures that two nodes agree that they are attached to the same body, that is, they sense the same ECG data. The proposed system utilized ECG Inter-Pulse-Intervals (IPI) between peaks as a unique feature extracted for the authentication purposes.

Table 2: Summary of ECG based biometric security solutions for healthcare using BANs

Proposed scheme [Reference]	**Security Measure**	**ECG feature**	**Performance**	**Limitations/ Future Direction**
Efficient ECG-based authentication scheme[118]	Key authentication	Vector of biometric features	FRR, FAR strong security against several attacks	• To improve feature extraction method • Explore features from other physiological signals such as PPG, EMG and ECC or a combination of them. • To perform analytical modeling of proposed protocol ECG-AS including expansion of the attack model
MFBSG algorithm[117]	BSEs encryption or authentication	IPIs (RR, RQ, RS, RP and RT intervals)	Latency	• Method was evaluated only from healthy subject databases, lacks robustness to handle abnormal datasets
GMM-based stochastic authentication Scheme[114]	stochastic authentication	IPI signals	FRR, FAR, and HTER	• low sample resolutions and small number of Gaussian mixtures under poor sample synchronization conditions were used
BodyKey methods[111]	symmetric key distribution	RR interval values	EER, FAR, FRR, communication, energy consumption	• Only a single public dataset was used therefore not practically robust. • More physiological properties such as ABP and Photoplethymography (PPG) can be explored
Vitacode Scheme[113]	key generation and distribution	IPI (inter-pulse interval), RR values and TT values	PhysioBank database, ERR of 2.66%	• Plan to explore practical ECG cryptosystem using the VitaCode representation for secure communications in BANs. • Only a single public dataset was used
AC/DCT -Based Fuzzy Vault Method[19]	Entity Identification for authentication	Frequency domain features.	FRR FAR, HTER	• Need to use smaller development board to deploy WBSN. • Limited number data was used • To embed biosensors onto the small development board to collect multiple bio signals using single sensor
Heartbeats based RBSs technique[28]	RBSs for key Agreement and encryption	Inter-pulse intervals (IPIs)	Processing time	• Up to 16 bits can be extracted from each heartbeat to achieve more optimal performance. • Need to strike a balance between the randomness and distinctiveness of 128-bit RBSs. • To designing adaptive RBSs generation model using heartbeats of different subjects
Certificateless biometric authentication scheme and group key management[120]	Authentication and group key management	Time-related and amplitude-based features	Strong security, storage overhead, computation cost and communication cost.	• Further security analysis on more robust security attacks can be conducted • Dataset is from healthy subjects only

ECG-based TRNG[119]	Authentication protocol	ECG window	Throughput, Efficiency	• Dataset was gotten from healthy subjects only. • Test the model with other biosignals • Further study on the entropy extraction problem in a transformed domain.
ECG-IJS key agreement scheme[115]	Key authentication	Time-variant ECG features	FAR, FRR, communication overhead, energy efficiency	• Performance can be improved by using more unique features for individuals and by adopting the optimal vault size and optimal difference tolerances
ECG-based authentication protocol[116]	Authentication protocol	Q-IPI, R-IPI and or S peaks (S-IPI)	FRR, FAR	• There is need for validation of the protocol using more subjects in different situations and abnormal ECG properties • Generation of secure session keys to enhance system performance
Fuzzy encryption and fuzzy vault technique[109]	Key authentication	QRS, PR and QT interval	True positive, False-positive, energy consumed	• Need to enhance communication protocol, the physical layer and routing protocol to improve system performance
Authentication and key agreement scheme[12]	Authentication and key agreement protocol	ECG signals	Computational overhead, communication overhead	• Suffers Computational overhead

Random Number Generators is a critical component in tasks such as the generation of a fresh session key or a set of random numbers for an authentication protocol in wireless sensor networks[119]. ECG feature values exhibit the property of randomness, and thus can be utilized to generate random binary sequences (RBSs), and are used for facilitating symmetric key distribution, authentication or as symmetric keys directly, in a study conducted in [117], ECG Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm was proposed. Unlike the existing algorithms that use Inter-pulse Intervals (IPIs) from each heartbeat cycle to process RBSes, which was found to consume a lot of time for real time monitoring, MFBSG algorithm used multiple fiducial points thereby reducing the latency. These randomly generated ECG RBSes can be used as security keys for encryption or authentication or be used to facilitate key distribution in a WBAN system. A study by [19] proposed a Discrete Cosine Transform (DCT) of the AutoCorrelation (AC) sequence based Fuzzy vault scheme, an Intel Galileo based WBSN platform which used ECG captured from human body for entity identifications (EIs) to authenticate data in WBSNs. A study conducted by [118] proposed a secure and efficient ECG-based scheme for authentication in Medical Body Area Sensor Networks (MBASNs). The scheme enables each pair of sensor nodes to exchange an encryption-key using the Elliptic Curve Die-Hellman (ECDH) protocol. ECDH however, does not guarantee the authentication during the exchange of keys process, hence the integration of an authentication phase using ECG signals to ensure that only the sensor nodes of the same MBASN can access patient's data. The authentication is performed using vector of biometric features which was formed by concatenating binary strings from integral computation which was gotten from ECG windows that passed through Fast Fourier Transformer (FFT). Security analysis of the proposed schemes prove promising to mitigate several attacks such as brute force attack, Sybil attack, session hijacking attack, man in the middle attack and impersonation attack. Another heartbeats based RBSs using IPIs of ECG signals was proposed by [28]. The technique incorporates finite monotonic increasing sequences generation mechanism of IPIs and cyclic block encoding procedure that extracts a high number of entropic bits from each IPI. Using the proposed technique, most 16 random bits can be extracted from each heartbeat to generate 128-bit RBSs via concatenation of eight consecutive IPIs which can potentially be used as keys for encryption or entity identifiers to secure WBSNs. The proposed technique achieved a real-time processing time (0-8 seconds). In another study, [119] proposed a True Random Number Generators (TRNGs) which is based on ECG which can be used to generate random numbers. The authors used ECG signals which is a true physiological elements found in every human to generate random numbers for authentication purpose in wireless sensor network. A secure certificateless biometric authentication scheme and group key management for WBANs scenarios was proposed by [120]. ECG signals was used for authentication where it achieved an efficient continuous authentication towards participating sensors using an efficient Group key distribution with dynamic updating mechanism. The authors claimed to be the first to combine the ECG signal with novel certificateless authentication strategies for resource-limited WBANs. The proposed approach achieved strong security properties and efficient in countering attacks such as chosen message attack, replay attack, illegal tracing and also achieved great improvement in storage overhead, computation cost and communication cost. In a study by [109] proposed a biomedical based fuzzy vault scheme for a secured authentication scheme for Body Sensor Network. A bio-metric key authentication scheme based on

ECG features such as peak points, time and gradient of the signal was proposed. Fuzzy encryption and fuzzy vault technique were used to encrypt and store data securely at the base station server against tempering. How it works? Any request to access the stored data, then the proposed fuzzy extractor process the data securely and the fuzzy vault is generated to activate the authentication key for accessing the data stored in the base station server with much security.

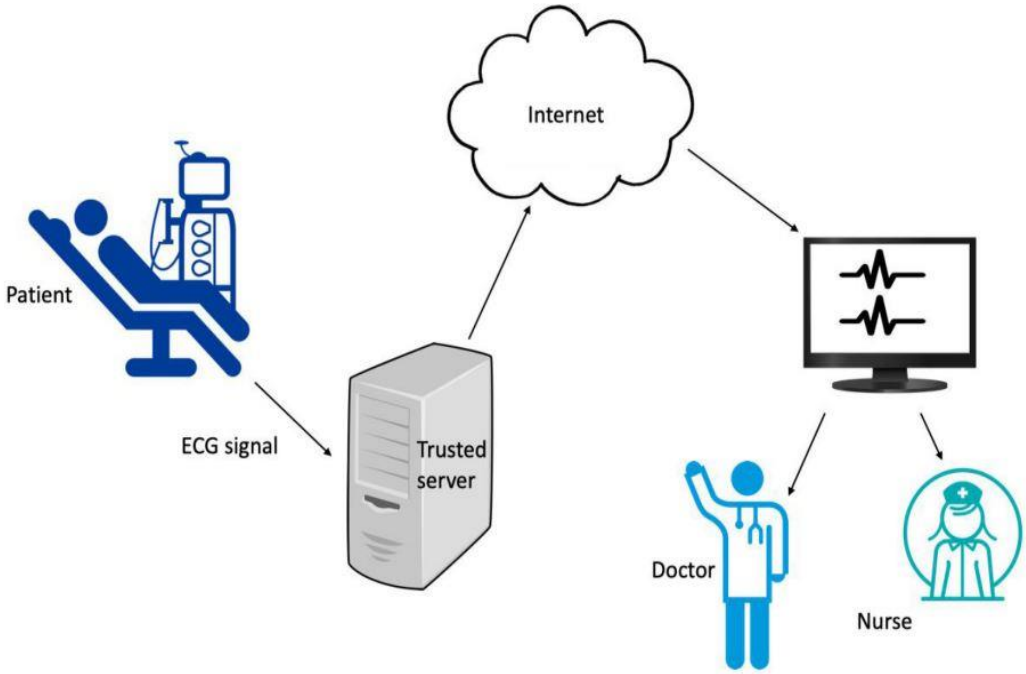

Fig. 5: Showing a typical wearable medical sensor network framework

Fig. 5 shows a framework of wireless wearable medical sensor which enables continuous monitoring of patients by the Doctors and Nurses in real-time [12]. The monitoring is dynamic such that the patients can continue actively in their day-to-day activities while being tracked by Doctors and Nurses at real time. Conversely, Doctors and Nurses can log on to their application to access the current readings of the physiological data being monitored. The security of this kind of remote monitoring system has been the major challenge to healthcare institutions. This led to different strategies proposed in the literature to ensure patients data are not hijacked or exposed to third party. Long-term secret keys and smart cards were introduced to supplement passwords and create two-factor user authentication schemes, but these methods were found to be vulnerable to impersonation once the attacker successfully guesses the password. Biometric keys were introduced due to the inefficiency of the previous methods, however, traditional biometrics provide static authentication which is vulnerable once the attacker gain access, they can own it without the need to re-authenticate. To address the issues of the traditional biometrics, continuous authentication were introduced through the use of human physiological signals such ECG, PPG, EEG to authenticate individual. However, previous methods [12] proposed an ECG based lightweight static and continuous mutual authentication and key agreement protocol. The protocol protects data privacy and provide mutual authentication between the doctor/nurse, trusted server, sensor and patient. The proposed approach was found resistant to so many security attacks including, user and sensor impersonation, physical sensor theft, replay attack and more. Table 2 provides the summary.

C. ECG based steganography systems for healthcare applications

Due to the advancement in technology, patient biosignals such as ECG can be acquired and transmitted over the internet for diagnosis and storage. The biosignals are usually trapped with the patient's identity information and it becomes the responsibility of the health care provider to maintain the privacy of patient information during such transmission [121]. Steganography is referred to as the process of hiding the secret data or information (watermark) within the cover image (host data). These secrets information such as patient name, age, address, allergy, medical condition etc, are the watermark whereas the bio-signals such as ECG and PPG are the cover image or host signals. Embedding the watermark into the cover signal may leads to deterioration of the host signal and that might affect its diagnosability.

A wavelet-based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data using ECG signal[80]. The proposed method demonstrates effectiveness to hide patient confidential data and other physiological information while at the same time keep the ECG signal (the host data) diagnosable. Figure 6 shows a scenario of steganography in point of care systems where different readings such as blood pressure, glucose, temperature as well as ECG signals are collected and watermarking is applied on them inside the patient's mobile phone[80].

ISSN No:-2456-2165

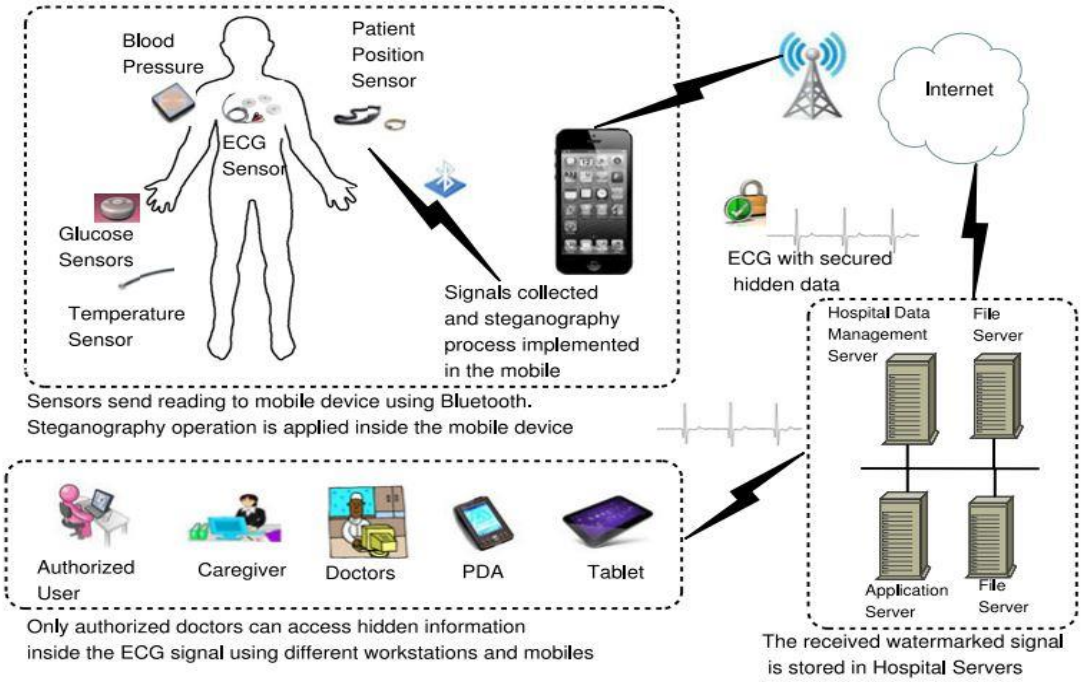

Fig. 6: ECG steganography scenario in Point-of-Care (PoC) systems

A study by [121] proposed ECG steganography using Discrete Wavelet Transform (DWT) and Quick Response code (QR) to minimize the deterioration of ECG signals and to preserve diagnosability. The converted data using QR code was used as watermark in ECG steganography. The proposed method allows reliable patient data protection with full retrieval ability. Table 3 presents the summary of these schemes.

Table 3: Summary of ECG steganography proposed schemes for healthcare applications

Proposed model [Reference]	Security measures	ECG feature	Performance Parameter	Limitations/ Future Direction
DWT + QR steganography technique[121]	Steganography	ECG signals	PSNR PRD	• The resilience of the proposed method against attack was not evaluated
Wavelet-based steganography technique[80]	Steganography & encryption	ECG signals	watermarked ECG can be used for diagnoses and the hidden data can be totally extracted	• Diagnosability of ECG signals was tested only by medical experts with no evidence of empirical analysis

D. Multimodal ECG-based biometric for healthcare applications

There are methods that considered a hybridization of physiological signals for a stronger and a robust authentication system. These proposed methods argue that the use of single ECG biometric system may not be sufficient to combat attacks and may suffer attacks due to computation power there is available [56, 122]. Hence, the fusion of two or more physiological modalities can enhance the strength of the security against stronger attacks. More so, the fact that not all patients can be expected to have normative cardiac signals due ailments may affect the cardiac process and by implication, affect the ECG-based biometric systems[32, 123].

Table 4: Summary of Multimodal biometric for healthcare application

Proposed model [Reference]	Security measure	Features [Type of Signal]	Performance parameter	Limitations/ Future Direction
LSTM[124]	Authentication	Instantaneous Frequency, spectral entropy [**ECG & PPG**]	PPG model better than ECG model with F1 score 1.00 and 0.86 respectively	• Limited number of dataset were used • ECG and PPG data of various posture and activities should be considered. • Multivariate authentication by combining ECG and PPG can be explored
Principal Component	Identification	ECG and ABP signals [**ECG & APB]**	Accuracy	• Model can be improved by reducing time for model training and increase dataset for training

Analysis (PCA)[123]				
CloudIoTPersonalCare[125]	Authentication	Frequency and spectral entropy features [**ECG & PPG**]	Accuracy	• Need to validate the end to end security aspects of the proposed model. • Limited number of users was used. • Data gotten from users at sitting postures only
LSTM, CNN, NB, GAM[32]	Authentication	WPT, AR, IF and SE [**ECG & PPG**]	Accuracy, EER	. More checks needed for other security attacks

A study presented by [123], proposed a patient identity verification approach based on the fusion of ECG with arterial blood pressure (ABP) to identify an individual patient. Instead of relying on the feature extraction from ECG and ABP which is often difficult and error prone, the authors removed the need for finding characteristic features when using ECG and ABP signals in tandem for identification of individuals. The proposed approach achieved 97% and 99% accuracy in identifying patients with non-normative cardiac rhythms and morphology and for patients whose cardiac rhythms are normative, respectively. Chronic diseases demand continuous monitoring and observation to keep track of the health status of a patient. Dementia is one such kind of disease, however, due to progressive and frequent memory loss and confusion, patients with Dementia face significant challenges to access medical services, hence the need for a support system. Another study conducted by [124] proposed a biometric-based authentication framework based on a recurrent neural network (LSTM) for dementia patients. They proposed model used ECG and PPG as the biometric traits for the system. The proposed model used a multi-step authentication by first authenticating a subject by ECG, if not successful, PPG is tested and if all failed, password option is activated. Comparatively, PPG based authentication model performed better than ECG authentication model for the selected dataset with F1 score 1.00 and 0.86 respectively. In [32], a deep-learning Long Short-Term Memory (LSTM) multimodal biometric-based authentication model that comprises continuous single and group user and device authentication in personalized healthcare network environments was proposed. The authors employ the use of machine learning and deep learning methods such Naive Bays, Ensemble, Generalised Additive Model (GAM), CNN and LSTM, using five different datasets. The proposed method combined features from a few common biometric traits such as ECG and PPG which was used to authenticate individual. Biometric Identity Management Framework based on the fusion of ECG and photoplethysmogram (PPG) signals was proposed in[125] for authentication and to ensure security and privacy of patients in personalized healthcare systems. Homomorphic Encryption was used to encrypt both the biometric parameters and patient data to preserve the confidentiality of the patients' data. The proposed fused-based biometric framework was successful in identifying and authenticating all 25 users with 100% accuracy. Table 4 present the summary of these schemes proposed in this section.

V. DISCUSSIONS, CHALLENGES AND OPEN RESEARCH OPPORTUNITIES

This section, presents discussion based from the review and other general challenges and research opportunities from the literature.

A new paradigm of Doctor-Patient relationship in healthcare systems was born with the advent and incorporation of IoTs and cloud computing technologies in healthcare sector. The integration of these technologies complements each other's capabilities when integrated as flexible, scalable and efficient patient healthcare systems. IoTs and cloud computing enhances electronic health (e-health) which is a superset of medical informatics, public health and Internet health services that embrace and drive the worldwide development of new technology to solve deep-rooted problems, minimize costs and enhance patient care [2, 3]. The ubiquity nature of IoTs has enabled the integration and interconnection of different "Things" to work seamlessly as a one big technological architecture. Different health IoT-enabled innovations emerged such as IoMTs, biosensors and WBANs devices which are based on using various smart medical devices connected within the network through the internet that are capable of collecting vital elements of the human body such as PPG, temperature, ABP and ECG for easy remote patient monitoring and diagnosis. IoTs based healthcare devices and applications are expected to monitor patient by gathering the vital data and transmitting it to other sources for remote monitoring and diagnosis. If they fail, the patient's life is at risk. Thus, it is expedient that security and patient privacy have higher priority in powering such technologies [56]. The security of healthcare applications is critical as it comprise the sensitive data of patients. Security of patients' personal record and access to health information systems has continued to be a cause of concern for both patients and health institutions.

Biometric systems are among the various techniques that have been proposed to handle the security of patients' personal data within the healthcare institutions [30]. Over the years, researchers have come to establish that ECG-based biometric approaches to the security of transmitted and stored patients' personal data have standout as the most convenient and effective approach. The features of ECG such as continuous, aliveness and internal nature are highly promising and suitable for healthcare systems compared to traditional biometrics[75]. More so, while using the ECG signals for security purposes, the diagnosis of the patient's cardiovascular health can also be performed with it[76], thereby, achieving dual purposes. ECG signal is not only a

ISSN No:-2456-2165

gold standard cardiac signal, but also unique to each individual[79]. Traditional biometric systems require extra hardware to be used in health care systems. As ECG of a patient is taken in the hospitals, the same can be used for identification without extra hardware[89]. According to Deshmane and Madhe [89] ECG based biometric can be mainly used in IoTs based health care systems where data is transferred on internet.

RQ1: *What are the ECG-based biometric schemes designed to provide security and privacy of patients' data in healthcare institutions?*

Research question 1 (RQ1) seeks to reveal the different ECG-based biometric schemes and algorithms proposed in the included papers that were used to improve the security and privacy of patients' data. Section 4.1, 4.2, 4.3 and 4.4 present brief discussions of the proposed schemes which were used to improve the performance of security and privacy of patients' medical records and identity, respectively, which range from statistical, fuzzy, probabilistic, stochastic and machine learning algorithms. Table 1, 2, 3 and 4 presents the summaries of these techniques proposed including the reference, proposed method, security measure/solution, ECG features, performance parameter, limitations and future directions as discovered and suggested in the reviewed papers.

RQ2: *What are the security and privacy measures/solutions achieved using ECG signals in the proposed schemes?*

The research question 2 (RQ2) put forward in this review seeks to uncover the security and privacy measures/solutions achieved using ECG signals in the proposed schemes as reviewed in this study. This review presents a systematic review of 45 primary studies that proposed security schemes for securing patients access to medical services and patients' data transmission in health institutions. Based from the reviewed papers, the following techniques were used to provide security of patients' data and to authorized individuals accessing medical services in healthcare environment, all powered by IoTs and cloud computing technologies.

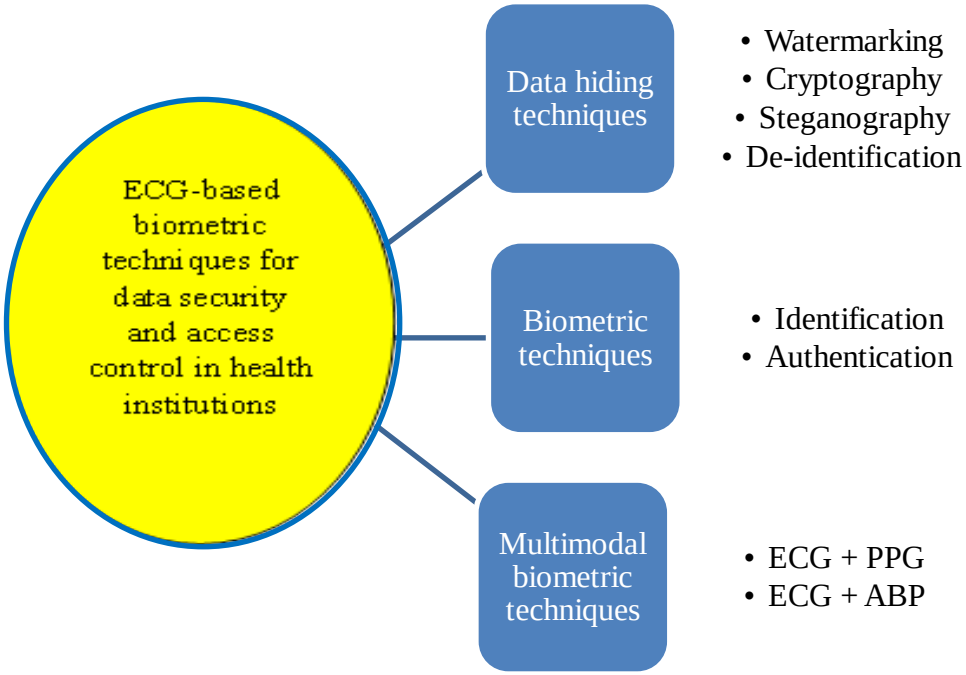

Fig. 7: Taxonomy of ECG-based biometric techniques for healthcare security

A. ECG-based biometric techniques:

Biometric systems either identifies or authenticates subjects based on their unique behavioral or physiological traits [44, 45]. ECG signals was first introduced by the U.S military as a biometric trait [69]. And the ECG features were found to be applicable and unique to individual as a biometric trait for human identification [70-72]. Based on this review, methods were proposed to identify and authenticate individuals for the purpose of diagnoses and granting access to medical applications using ECG (Table 1). The challenge of using ECG signals for biometric is the fact that not all humans are healthy; there are those suffering from one cardiac disease or the other which may affect the normal rhyme and beat rate of the ECG signals and by implication, affect the identification and authentication performance of the ECG-based biometric systems [102, 123]. Therefore, ECG-based biometric systems have to be evaluated on datasets from both healthy and unhealthy individuals in order to verify their robustness in identifying subjects[103]. The ECG biometric identification and authentication systems' performance reported in the literature varies depending on databases used, methods of ECG data recording, sample size, signal pre-processing techniques, types of feature extraction, and classification model [88]. Based on the studies on ECG biometric systems, generally, it shows that different ECG features were best fit for some models better than the other ECG features from the same source body. Further studies on selecting the best, stable and salient ECG features to be applied for ECG biometric will go a long way to enhance the accuracy of ECG biometric systems. The selection of

ISSN No:-2456-2165

relevant and important features has a significant effect on the performance of a classification model's performance[126]. Even though ECG based biometric authentication system provide good accuracy, in practice, ECG-based authentication may be far from being accurate because ECG recording is always contaminated by noise and artifacts [98]. Even the same ECG monitored at the same time from different locations of the same body will give variations to a certain extent [113]. Factors that affect the ECG waveform can be classified as physiological or psychological[7]. According to Agrafioti et al. [7] emotional activity can compromise the stability and robustness of a biometric template and significant enough to endanger biometric system accuracy.

B. ECG-based biometric data hiding techniques:

Data hiding techniques are the schemes that hide data by way of encryption, scrambling, watermarking and disguising such that an intruder finds it difficult to decode the massage (data) being transmitted. Different techniques have been proposed in the literature to hide data, which include cryptography, watermarking and steganography[127, 128]. Cryptography involves converting message with a key and transform it into a cipher text which the receiver of the message use the key to decrypt it. Cryptography can be divided based on the key used to encrypt and decrypt the messages. Public key cryptography also called asymmetric cryptography uses different keys to encrypt and decrypt the massage, private key or symmetric cryptography use a single key to encrypt and decrypt the messages while hash function cryptography uses a fixed length hash value based on the plain text which are used to encrypt passwords. Shi and Lam [113], proposed a method vitacode which extract ECG features and were used to produce some structure representation and a fuzzy cryptography was used to distribute the keys. In another study, Shi, Lam and Gu [111] proposed a method to generate and distribute keys using the biometric ECG, and ensure the biomedical sensors deployed on the genuine body can possess the exact keys by an inexpensive mechanism using biometrics. Steganography hides sensitive data into insensitive one which is called the host or cover data. The sensitive data is embedded into the cover image and transmit it over to the sender. Steganography was demonstrated by [80, 121] where ECG signals serves as the host data which hides the sensitive data effectively. The sender can extract the message with the help of a key. Watermarking is a process of inserting information otherwise called the watermark in the image either visibly or invisibly such that any attempt to claim ownership will be invalid. However, embedding the watermark (sensitive data) into the host data may leads to deterioration of the host signal and that might affect its diagnosability.

Another form of data hiding is de-identification process. De-identification simply involves the removal of any traceable identifier in a data and transmit the data over the network such that no would detect the owner of the data. Instead of relying on the ECG biometric identification of individuals from healthy and unhealthy population or datasets, there are methods that attempt to de-identify ECG signals such that it will be hard or impossible to detect whose ECG signal is being transmitted over a network [108]. In a novel study, [108] proposed a method to de-identify ECG signals using a Generative Adversarial Network (GAN)-based framework while at the same time, preserving ECG signal structure and the target cardio vascular condition information.

Generally, the use of ECG signals in cryptography, watermarking, steganography and de-identification comes with the challenge of protecting the ECG signals itself and maintain it diagnosability. It's pertinent to note that while using ECG signals to protect patient data, the ECG signal itself has to be protected. Also, precautions to take while encrypting ECG signals is to make sure it can be decrypted back to its original signals to enable diagnosablitiy of the signals. The proposed methods demonstrate effectiveness to hide patient confidential data and other physiological information while at the same time keep the ECG signal (the host data) diagnosable after hiding patient confidentiality [80, 96, 108, 121].

C. Multimodal biometric techniques:

The use of single ECG physiological signal may not be robust enough to combat attacks [56, 122]. Hence, researchers have proposed the fusion of two or more physiological modalities to enhance the strength of the security against stronger attacks. A study by [32, 124, 125] fused ECG and PPG for identification and authentication purposes, [123] fused ECG and ABP for identification of individual patient. The reasons behind the use of ECG or PPG are twofold, the biosensors which are used to collect remote health data from patients can measure ECG and PPG of a patient easily, and they are hard to forge by an impostor [124]. Therefore, they do not require extra hardware to collect them.

Some other inherent and open research challenges associated with ECG biometric systems for remote patient monitoring systems include;

- **Insufficient data for training models:** There is a problem with insufficient data for training of models, especially for data-hungry models like deep learning models. There is generally, a limited datasets for ECG biometric systems compared to large repository of fingerprint datasets. Table 1, 2, 3 and 4 revealed limitations of insufficient data for training of some models. Insufficient training data may affect the models' generalization. The limited ECG biometric datasets, the problem induced by various cardiac diseases which affect the ECG signal quality and the variations of ECG signals under physical activities or changes due to cardiac defense mechanism present a challenge which affects generalization ability of the identification and authentication algorithms [102]. A comparative performance of identification system based from dataset of healthy individuals was better than to those diagnosed with cardiovascular diseases [103]. This is as a result of dramatic change over time of ECG signals collected from subjects diagnosed with CVDs compared to those from healthy ones. More ECG signals from different session of recording are needed to improve the identification accuracy[40].

ISSN No:-2456-2165

- **Design considerations of remote patient monitoring sensors and applications.** The development of low-cost ECG devices and lightweight applications is necessary for remote patient monitoring systems such as the use of resource-constrained (limited power, limited processing, and limited memory) medical sensors and applications [73, 97]. Due to resource-constrained of IoMT nature of sensor nodes, development of an efficient security mechanism is vital, which could accurately use the resources of the system. IoMTs is a building block for modern healthcare having enormously stringent resource constraints thus lightweight health data security and privacy are crucial requirements [97]. The lack of energy resources, computation and storage of the sensors presents a hard challenge, which should be addressed by establishing a tradeoff between the security and the efficiency[118]. In BANs schemes, several considerations should be taken into cognizance during the design of the systems and sensors such as method of ECG extraction should aim at reducing the latency (time it takes to extract the features). The transmission of data over the communication networks should ensure low computational cost (communication overheads), storage overheads, bandwidth (processing time), and minimal energy consumption. Treatment should not be delayed especially in case of emergency[118]. Also, location features for the patients in remote patient monitoring systems can be improved by incorporating Global Positioning System (GPS) support, especially in the real-time monitoring of ECGs patients in ambulatory settings for location-based continuous surveillance and monitoring[73].

VI. CONCLUSIONS

This paper systematically reviewed the various ECG-based biometric schemes proposed to mitigate security and privacy issues in healthcare institutions. The security and privacy of individual's data is non-negotiable in every data-driven institution, especially in healthcare institutions. This study revealed ECG-based biometric schemes which were used to provide security and privacy of patients' medical records and also to verify identity of users accessing medical services, which range from statistical, fuzzy, probabilistic, stochastic and machine learning algorithms. More so, taxonomy of security and privacy measures/solutions achieved using ECG-based biometric schemes from the reviewed papers was presented. ECG as a biometric modality has proven to be more robust against security attacks better than the traditional biometrics with unique features such as possession of continuous, aliveness and internal nature properties which makes it suitable and unique for providing security and privacy in healthcare remote monitoring system. Different security solutions such as data hiding techniques using ECG signals for creating cryptographic messages, creating digital watermarks, serves as a cover data in steganography and performing de-identification on the ECG signal to provide anonymity of ECG signals were discussed. Also, the fusion of ECG with other physiological modalities such as PPG and ABP to enhance the strength of the security against stronger attacks was also presented in the study.

Challenges and research opportunities were discussed to enable novel researches. Further studies should consider developing ECG-based biometric schemes that are sensitive to the dynamics of ECG signals, location of patients and complexity of the medical sensors. We are confident that this study will be a great resource for researchers who want to advance the performance of the security techniques for patients' data and identity verification using ECG signals in the future.

ACKNOWLEDGEMENT

We wish to acknowledge the Tertiary Education Trust Fund (TETFUND) for providing the team with the Institution Based Research (IBR) grant which was used in funding the research.

REFERENCES

[1.] Sikder, A., et al., *A survey on sensor-based threats to internet-of-things (IoT) devices and applications. arXiv 2018.* arXiv preprint arXiv:1802.02041, 2018.

[2.] Butpheng, C., K.-H. Yeh, and H. Xiong, *Security and privacy in IoT-cloud-based e-health systems—A comprehensive review.* Symmetry, 2020. 12(7): p. 1191.

[3.] Agarwal, S. and D. Dasaya, *IoT-Based ECG Monitoring System for Health Care Applications.* Mathematical Statistician and Engineering Applications, 2022. 71(4): p. 10375-10391.

[4.] Kailas, A. and M.A. Ingram. *Wireless communications technology in telehealth systems*. in *2009 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*. 2009. IEEE.

[5.] Solanas, A., et al., *Smart health: A context-aware health paradigm within smart cities.* IEEE Communications Magazine, 2014. 52(8): p. 74-81.

[6.] SC, S., K. V, and G. VK, *Telecardiology for effective healthcare services.* Journal of medical engineering & technology, 2003. 27(4): p. 149-159.

[7.] Agrafioti, F., F.M. Bui, and D. Hatzinakos, *Secure telemedicine: Biometrics for remote and continuous patient verification.* Journal of Computer Networks and Communications, 2012. 2012.

[8.] Rheuban, K., *Telehealth and telemedicine technologies: Overview, benefits, and implications.* Systems engineering approach to medical automation. Boston: Artech House Publishers, 2009.

[9.] Khemapech, I., W. Sansrimahachai, and M. Toachoodee, *Telemedicine–meaning, challenges and opportunities.* Siriraj medical journal, 2019. 71(3): p. 246-252.

[10.] Livinsa, M.Z., et al., *E Health Monitoring Systems in Smart Environments.* Journal of Pharmaceutical Sciences and Research, 2019. 11(9): p. 3130-3132.

[11.] Kotevski, A., N. Koceska, and S. Koceski, *E-health monitoring system.* 2016.

[12.] Ying, B., N.R. Mohsen, and A. Nayak, *Efficient authentication protocol for continuous monitoring in*

medical sensor networks. IEEE Open Journal of the Computer Society, 2021. 2: p. 130-138.
[13.] Boikanyo, K., et al., *Remote patient monitoring systems: Applications, architecture, and challenges.* Scientific African, 2023: p. e01638.
[14.] Newaz, A.I., et al., *A survey on security and privacy issues in modern healthcare systems: Attacks and defenses.* ACM Transactions on Computing for Healthcare, 2021. 2(3): p. 1-44.
[15.] Suraki, M.Y. and M. Jahanshahi. *Internet of things and its benefits to improve service delivery in public health approach.* in *2013 7th International Conference on Application of Information and Communication Technologies*. 2013. IEEE.
[16.] Singh, R.P., et al., *Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications.* Journal of clinical orthopaedics and trauma, 2020. 11(4): p. 713-717.
[17.] Wu, W., S. Pirbhulal, and G. Li, *Adaptive computing-based biometric security for intelligent medical applications.* Neural Computing and Applications, 2020. 32: p. 11055-11064.
[18.] Yaghoubi, M., K. Ahmed, and Y. Miao, *Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges.* Journal of Sensor and Actuator Networks, 2022. 11(4): p. 67.
[19.] Pirbhulal, S., et al. *A comparative study of fuzzy vault based security methods for wirless body sensor networks*. in *2016 10th International Conference on Sensing Technology (ICST)*. 2016. IEEE.
[20.] Zhang, M., A. Raghunathan, and N.K. Jha, *Trustworthiness of medical devices and body area networks.* Proceedings of the IEEE, 2014. 102(8): p. 1174-1188.
[21.] Kamalov, F., et al., *Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective.* Sustainability, 2023. 15(4): p. 3317.
[22.] Srivastava, J., et al., *Internet of Medical Things (IoMT)-based smart healthcare system: Trends and progress.* Computational Intelligence and Neuroscience, 2022. 2022.
[23.] Sobya, D., et al., *Wireless ECG monitoring system using IoT based signal conditioning module for real time signal acquisition.* Indian J. Public Health Res. Dev, 2018. 9: p. 294-299.
[24.] La Pietra, L., et al., *Medical errors and clinical risk management: state of the art.* Acta otorhinolaryngologica italica, 2005. 25(6): p. 339.
[25.] Choudhury, L.S. and C.T. Vu, *Patient identification errors: A systems challenge.* Patient Safty Network PSNet, 2020.
[26.] Mbonihankuye, S., A. Nkunzimana, and A. Ndagijimana, *Healthcare data security technology: HIPAA compliance.* Wireless communications and mobile computing, 2019. 2019: p. 1-7.
[27.] Serhani, M.A., et al., *ECG monitoring systems: Review, architecture, processes, and key challenges.* Sensors, 2020. 20(6): p. 1796.
[28.] Pirbhulal, S., et al., *Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks.* IEEE Transactions on Biomedical Engineering, 2018. 65(12): p. 2751-2759.
[29.] Chen, H., et al. *Security design of ECG telemonitoring systems*. in *2020 International Conference on Computer Engineering and Application (ICCEA)*. 2020. IEEE.
[30.] Singh, A.K., et al., *A survey on healthcare data: a security perspective.* ACM Transactions on Multimidia Computing Communications and Applications, 2021. 17(2s): p. 1-26.
[31.] Hathaliya, J.J. and S. Tanwar, *An exhaustive survey on security and privacy issues in Healthcare 4.0.* Computer Communications, 2020. 153: p. 311-335.
[32.] Ahamed, F., et al., *An intelligent multimodal biometric authentication model for personalised healthcare services.* Future Internet, 2022. 14(8): p. 222.
[33.] Thamer, N. and R. Alubady. *A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research*. in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. 2021. IEEE.
[34.] Silva, H., et al. *Clinical data privacy and customization via biometrics based on ECG signals*. in *Symposium of the Austrian HCI and Usability Engineering Group*. 2011. Springer.
[35.] Mohamed, T.S., *Security of Multifactor Authentication Model to Improve Authentication Systems.* Information and Knowledge Management. ISSN, 2014: p. 2224-5758.
[36.] Mohammed, S., L. Ramkumar, and V. Rajasekar, *Password-based Authentication in Computer Security: Why is it still there.* The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), 2017. 5(2): p. 33-36.
[37.] Conklin, A., G. Dietrich, and D. Walz. *Password-based authentication: a system perspective*. in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. 2004. IEEE.
[38.] Aboud, S.J., *Secure password authentication system using smart card.* International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2014. 3(1): p. 75-79.
[39.] Jiang, Q., et al., *Improvement of robust smart-card-based password authentication scheme.* International Journal of Communication Systems, 2015. 28(2): p. 383-393.
[40.] Jyotishi, D. and S. Dandapat. *Person Identification using Spatial Variation of Cardiac Signal*. in *2020 IEEE Applied Signal Processing Conference (ASPCON)*. 2020. IEEE.
[41.] Le, C. and R. Jain, *A survey of biometrics security systems.* EEUU. Washington University in St. Louis, 2009.
[42.] Sabhanayagam, T., V.P. Venkatesan, and K. Senthamaraikannan, *A comprehensive survey on various biometric systems.* International Journal of Applied Engineering Research, 2018. 13(5): p. 2276-2297.

[43.] Rathod, V.J., N.C. Iyer, and S. Meena. *A survey on fingerprint biometric recognition system*. in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2015. IEEE.
[44.] Pinto, J.R., J.S. Cardoso, and A. Lourenço, *Evolution, current challenges, and future possibilities in ECG biometrics.* IEEE Access, 2018. 6: p. 34746-34776.
[45.] Lynn, H.M., S.B. Pan, and P. Kim, *A deep bidirectional GRU network model for biometric electrocardiogram classification based on recurrent neural networks.* IEEE Access, 2019. 7: p. 145395-145405.
[46.] Salloum, R. and C.-C.J. Kuo. *ECG-based biometrics using recurrent neural networks*. in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2017. IEEE.
[47.] Bansal, R., P. Sehgal, and P. Bedi, *Minutiae extraction from fingerprint images-a review.* IJCSI International Journal of Computer Science 2011. 8(5): p. 74-85.
[48.] Bowyer, K.W., K. Hollingsworth, and P.J. Flynn, *Image understanding for iris biometrics: A survey*. Computer vision and image understanding, 2008. 110(2): p. 281-307.
[49.] Sarkar, I., et al., *Palm vein authentication system: a review.* International Journal of Control and Automation, 2010. 3(1).
[50.] Monrose, F. and A.D. Rubin, *Keystroke dynamics as a biometric for authentication.* Future Generation computer systems, 2000. 16(4): p. 351-359.
[51.] Hafemann, L.G., R. Sabourin, and L.S. Oliveira. *Offline handwritten signature verification—Literature review.* in *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*. 2017. IEEE.
[52.] Sarkar, A. and B.K. Singh, *A review on performance, security and various biometric template protection schemes for biometric authentication systems.* Multimedia Tools and Applications, 2020. 79(37): p. 27721-27776.
[53.] Alaswad, A.O., A.H. Montaser, and F.E. Mohamad, *Vulnerabilities of biometric authentication "threats and countermeasures".* International Journal of Information & Computation Technology, 2014. 4(10): p. 947-58.
[54.] Jain, R. and C. Kant, *Attacks on biometric systems: an overview.* International Journal of Advances in Scientific Research, 2015. 1(07): p. 283-288.
[55.] Mitchell, A.R., et al., *Electrocardiogram-based biometrics for user identification–Using your heartbeat as a digital key.* Journal of Electrocardiology, 2023.
[56.] Karimian, N., D.L. Woodard, and D. Forte. *On the vulnerability of ECG verification to online presentation attacks*. in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. 2017. IEEE.
[57.] Bhatnagar, S. and N. Mishra. *Conventional Biometrics and Hidden Biometric: A Comparative Study*. in *Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 2*. 2021. Springer.
[58.] Bhatnagar, S. and N. Mishra, *A Review of MRI Brain Print as Hidden Biometric.* TEST Engineering & Management, 2020. 83: p. 28571-28578.
[59.] Kulkarni, S., R. Raut, and P. Dakhole, *A novel authentication system based on hidden biometric trait.* Procedia Computer Science, 2016. 85: p. 255-262.
[60.] Ivanciu, L., P. Farago, and S. Hintea, *A review of ECG based biometric systems.* Acta Technica Napocensis, 2018. 59(4): p. 1-4.
[61.] Al Rahhal, M.M., et al., *Deep learning approach for active classification of electrocardiogram signals.* Information Sciences, 2016. 345: p. 340-354.
[62.] Park, J.Y., et al. *Deep ECG estimation using a bed-attached geophone*. in *17th ACM International Conference on Mobile Systems, Applications, and Services, MobiSys 2019*. 2019. Association for Computing Machinery, Inc.
[63.] Apandi, Z.F.M., R. Ikeura, and S. Hayakawa. *Arrhythmia Detection Using MIT-BIH Dataset: A Review.* in *2018 International Conference on Computational Approach in Smart Systems Design and Applications (ICASSDA)*. 2018. IEEE.
[64.] Agrawal, V., et al., *ElectroCardioGram (ECG)-based user authentication using deep learning algorithms.* Diagnostics, 2023. 13(3): p. 439.
[65.] Antczak, K., *Deep recurrent neural networks for ECG signal denoising.* arXiv preprint arXiv:1807.11551, 2018.
[66.] Banerjee, R., A. Ghose, and S. Khandelwal. *A Novel Recurrent Neural Network Architecture for Classification of Atrial Fibrillation Using Single-lead ECG*. in *2019 27th European Signal Processing Conference (EUSIPCO)*. 2019. IEEE.
[67.] Swapna, G., S. Kp, and R. Vinayakumar, *Automated detection of diabetes using CNN and CNN-LSTM network and heart rate signals.* Procedia computer science, 2018. 132: p. 1253-1262.
[68.] Zhou, X., et al. *A method of ECG template extraction for biometrics applications*. in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 2014. IEEE.
[69.] Forsen, G., M. Nelson, and R. Staron Jr, *Personal Attributes Authentication Techniques; Pattern Analysis & Recognition Corporation, Rome Air Development Center: St.* Utica, NY, USA, 1977.
[70.] Biel, L., et al., *ECG analysis: a new approach in human identification.* IEEE transactions on instrumentation and measurement, 2001. 50(3): p. 808-812.
[71.] Irvine, J.M., et al. *A new biometric: human identification from circulatory function*. in *Joint Statistical Meetings of the American Statistical Association, San Francisco*. 2003.
[72.] Shen, T.-W., W. Tompkins, and Y. Hu. *One-lead ECG for identity verification*. in *Proceedings of the second joint 24th annual conference and the annual fall meeting of the biomedical engineering society][engineering in medicine and biology*. 2002. IEEE.
[73.] Faruk, N., et al., *A comprehensive survey on low-cost ECG acquisition systems: Advances on design*

specifications, challenges and future direction. Biocybernetics and Biomedical Engineering, 2021. 41(2): p. 474-502.
[74.] Pereira, T.M., et al., *Biometric recognition: A systematic review on electrocardiogram data acquisition methods.* Sensors, 2023. 23(3): p. 1507.
[75.] Zhang, Y., et al., *PEA: Parallel electrocardiogram-based authentication for smart healthcare systems.* Journal of Network and Computer Applications, 2018. 117: p. 10-16.
[76.] Fuster-Barceló, C., C. Cámara, and P. Peris-López, *Unleashing the Power of Electrocardiograms: A novel approach for Patient Identification in Healthcare Systems with ECG Signals.* arXiv preprint arXiv:2302.06529, 2023.
[77.] Musa, N., et al., *A systematic review and Meta-data analysis on the applications of Deep Learning in Electrocardiogram.* Journal of ambient intelligence and humanized computing, 2022: p. 1-74.
[78.] Hong, S., et al., *Opportunities and Challenges in Deep Learning Methods on Electrocardiogram Data: A Systematic Review. arXiv 2019.* arXiv preprint arXiv:2001.01550, 2019.
[79.] Zhang, Q. *Phase-domain deep patient-ECG image learning for zero-effort smart health security*. in *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 2019. IEEE.
[80.] Ibaida, A. and I. Khalil, *Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems.* IEEE Transactions on biomedical engineering, 2013. 60(12): p. 3322-3330.
[81.] Chamatidis, I., A. Katsika, and G. Spathoulas. *Using deep learning neural networks for ECG based authentication.* in *2017 International Carnahan Conference on Security Technology (ICCST)*. 2017. IEEE.
[82.] Hammad, M., S. Zhang, and K. Wang, *A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication.* Future Generation Computer Systems, 2019. 101: p. 180-196.
[83.] Sarkar, A. and B.K. Singh, *A Review on Security Attacks in Biometric Authentication Systems.* International Research Journal of Engineering and Technology, 2018. 5(12): p. 1300-1304.
[84.] Xiao, Y. and M. Watson, *Guidance on conducting a systematic literature review.* Journal of planning education and research, 2019. 39(1): p. 93-112.
[85.] Keele, S., *Guidelines for performing systematic literature reviews in software engineering.* 2007, Technical report, ver. 2.3 ebse technical report. ebse.
[86.] Kitchenham, B., *Procedures for performing systematic reviews.* Keele, UK, Keele University, 2004. 33(2004): p. 1-26.
[87.] Brereton, P., et al., *Lessons from applying the systematic literature review process within the software engineering domain.* Journal of systems and software, 2007. 80(4): p. 571-583.
[88.] Tan, R. and M. Perkowski, *Toward improving electrocardiogram (ECG) biometric verification using mobile sensors: A two-stage classifier approach.* Sensors, 2017. 17(2): p. 410.
[89.] Deshmane, M. and S. Madhe. *ECG based biometric human identification using convolutional neural network in smart health applications*. in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. 2018. IEEE.
[90.] Qadri, Y.A., et al., *The future of healthcare internet of things: a survey of emerging technologies.* IEEE Communications Surveys & Tutorials, 2020. 22(2): p. 1121-1167.
[91.] Sriram, J.C., et al. *Activity-aware ECG-based patient authentication for remote health monitoring.* in *Proceedings of the 2009 international conference on Multimodal interfaces*. 2009.
[92.] Silva, H., et al. *Clinical data privacy and customization via biometrics based on ECG signals*. in *Information Quality in e-Health: 7th Conference of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society, USAB 2011, Graz, Austria, November 25-26, 2011. Proceedings 7*. 2011. Springer.
[93.] Huang, P., et al. *A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems*. in *2016 IEEE global communications conference (GLOBECOM)*. 2016. IEEE.
[94.] Chen, Y. and W. Chen. *Finger ECG-based authentication for healthcare data security using artificial neural network*. in *2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom)*. 2017. IEEE.
[95.] Al Alkeem, E., et al., *An enhanced electrocardiogram biometric authentication system using machine learning.* IEEE Access, 2019. 7: p. 123069-123075.
[96.] Zaghouani, E.K., A. Benzina, and R. Attia. *ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission*. in *2017 13th international wireless communications and mobile computing conference (IWCMC)*. 2017. IEEE.
[97.] Pirbhulal, S., et al. *Towards machine learning enabled security framework for IoT-based healthcare*. in *2019 13th International Conference on Sensing Technology (ICST)*. 2019. IEEE.
[98.] Huang, P., et al., *Practical privacy-preserving ECG-based authentication for IoT-based healthcare.* IEEE Internet of Things Journal, 2019. 6(5): p. 9200-9210.
[99.] Jyotishi, D. and S. Dandapat, *An Attention Based Hierarchical LSTM Architecture for ECG Biometric System.* 2021.
[100.] Behrouzi, P., B. Shirkani, and M. Hazratifard, *Using ECG Signals in Siamese Networks for Authentication in Digital Healthcare Systems.* Journal ISSN, 2022. 2766: p. 2276.
[101.] Sidek, K.A., H.F. Jelinek, and I. Khalil. *Identification of cardiac autonomic neuropathy patients using cardioid based graph for ECG biometric*. in *2011 Computing in Cardiology*. 2011. IEEE.

[102.] Zhang, Q., D. Zhou, and X. Zeng, *HeartID: A multiresolution convolutional neural network for ECG-based biometric human identification in smart health applications.* Ieee Access, 2017. 5: p. 11805-11816.
[103.] Chen, M., et al. *A comparative performance study of electrocardiogram-based human identity recognition*. in *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*. 2019. IEEE.
[104.] Wu, S.-C., P.-L. Hung, and A.L. Swindlehurst, *ECG biometric recognition: unlinkability, irreversibility, and security*. IEEE Internet of Things Journal, 2020. 8(1): p. 487-500.
[105.] Xu, G., *IoT-assisted ECG monitoring framework with secure data transmission for health care applications.* IEEE Access, 2020. 8: p. 74586-74594.
[106.] Camara, C., P. Peris-Lopez, and J.E. Tapiador, *Human identification using compressed ECG signals.* Journal of medical systems, 2015. 39: p. 1-10.
[107.] Tan, R. and M. Perkowski. *ECG biometric identification using wavelet analysis coupled with probabilistic random forest*. in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*. 2016. IEEE.
[108.] Jafarlou, S., et al. *ECG Biosignal Deidentification Using Conditional Generative Adversarial Networks*. in *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. 2022. IEEE.
[109.] Mahendran, R.K. and P. Velusamy, *A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things.* Computer Communications, 2020. 153: p. 545-552.
[110.] Darwish, A. and A.E. Hassanien, *Wearable and implantable wireless sensor network solutions for healthcare monitoring.* Sensors, 2011. 11(6): p. 5561-5595.
[111.] Shi, J., et al. *Towards energy-efficient secure communications using biometric key distribution in wireless biomedical healthcare networks*. in *2009 2nd International Conference on Biomedical Engineering and Informatics*. 2009. IEEE.
[112.] Jabeen, T., H. Ashraf, and A. Ullah, *A survey on healthcare data security in wireless body area networks.* Journal of ambient intelligence and humanized computing, 2021: p. 1-14.
[113.] Shi, J. and K.-Y. Lam. *VitaCode: electrocardiogram representation for biometric cryptography in body area networks*. in *2009 First International Conference on Ubiquitous and Future Networks*. 2009. IEEE.
[114.] Wang, W., et al., *Secure stochastic ECG signals based on Gaussian mixture model for $ e $-healthcare systems.* IEEE Systems Journal, 2011. 5(4): p. 564-573.
[115.] Zhang, Z., et al., *ECG-cryptography and authentication in body area networks.* IEEE Transactions on Information Technology in Biomedicine, 2012. 16(6): p. 1070-1078.
[116.] Peter, S., et al., *Design of secure ECG-based biometric authentication in body area sensor networks.* Sensors, 2016. 16(4): p. 570.
[117.] Zheng, G., et al., *Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks.* IEEE journal of biomedical and health informatics, 2016. 21(3): p. 655-663.
[118.] Zebboudj, S., et al., *Secure and efficient ECG-based authentication scheme for medical body area sensor networks.* Smart Health, 2017. 3: p. 75-84.
[119.] Camara, C., et al., *ECG-RNG: A random number generator based on ECG signals and suitable for securing wireless sensor networks.* Sensors, 2018. 18(9): p. 2747.
[120.] Tan, H. and I. Chung, *Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor.* IEEE Access, 2019. 7: p. 151459-151474.
[121.] Mathivanan, P., et al., *QR code based patient data protection in ECG steganography.* Australasian physical & engineering sciences in medicine, 2018. 41: p. 1057-1068.
[122.] Eberz, S., et al., *Broken hearted: How to attack ECG biometrics.* 2017.
[123.] Cai, H. and K.K. Venkatasubramanian. *Patient identity verification based on physiological signal fusion*. in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. 2017. IEEE.
[124.] Farid, F. and F. Ahamed. *Biometric authentication for dementia patients with recurrent neural network*. in *2019 International Conference on Electrical Engineering Research & Practice (ICEERP)*. 2019. IEEE.
[125.] Farid, F., et al., *A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services.* Sensors, 2021. 21(2): p. 552.
[126.] Luo, K., et al., *Patient-specific deep architectural model for ECG classification.* Journal of healthcare engineering, 2017. 2017.
[127.] Al-Yousuf, F.Q.A. and R. Din, *Review on secured data capabilities of cryptography, steganography, and watermarking domain.* Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 2020. 17(2): p. 1053-1059.
[128.] Kalita, M. and T. Tuithung, *A comparative study of steganography algorithms of spatial and transform domain.* International Journal of Computer Applications, 2016. 975: p. 8887.