Chapter

MedMetrics: Biometrics Passports in Medical and Clinical Healthcare That Enable AI and Blockchain

Huiqi Yvonne Lu

Abstract

The term biometrics was defined to suggest any measurable biological and biomedical metrics that can be used to identify and confirm the uniqueness of individuals. In this chapter, we would like to introduce an emerging area of biometrics, MedMetrics, that combines patient and drug information managed in coded passports to keep medical information accessible, safe and fraud-resistance. Medmetics includes medical and biological biometrics of patients based on their electronic health records, International Classification of Disease codes, Anatomical Therapeutic Chemical codes, Defined Daily Doses, time-series test results, and personalizsed biological data. By combining the blockchain technology, Medimetrics enables sensitive data sharing in between different clinical settings, allowing monitoring patients' health and care, as well as avoiding identification-related medical mistakes or frauds. MedMetrics Blockchain Passport can be used to identify patients and confirm their previous health conditions without the right of modifying or removing previous records. Medmetrics can revolutionary change the user demographic, shift safety restrictions, define new user applications, and encourage ethical AI regulations in medical science and health care. This chapter will discuss these directions and provide insights into the next generation of biometrics in medical science and health care.

Keywords: MedMetrics, biometrics, personal identity, healthcare, medical health record, NLP, BERT, ICD, blockchain, artificial intelligence

1. Introduction

Biometrics was traditionally referred to as a measurement that can help to identify an individual or to rule out intruders. From using fingerprint with ink on paper for a residence card in ancient China to using fingerprint on the digital optic scanner, from face recognition at door entry system to ECG identification for patients, the biometrics technologies have been re-defined in the last decade to fit the ever-increasing needs in advanced biometrics technologies. The latest developments were derived from the enormous boosting of personal mobile devices, the improved affordability of fingerprint sensors and CCTV cameras, the fast 4G and 5G communication network, and the increasingly successful cases of using biometrics in public and private sectors.

Generally speaking, a typical biometrics identification system will firstly record the physical or behavioural characteristics as the ground truth of personal identity, sometimes combine with personal information, e.g., name, gender, date of birth, address, and identification number if applicable. Secondly, a biometrics system will transform single or multiple biometrics and personal information into one encrypted code representing an individual. There is an algorithm to decide the similarity matrix among different codes. When a user attempts to get authorised by using a biometrics identification system, a decision threshold will be applied to decide whether to grant or deny the authorisation.

There are multiple agents within the organisational network to enable the processes of biometrics authorisation. For example, as shown in **Figure 1**, the Image Acquiring Agent is to collect biometrics information (in this example it is an iris image), the Iris Image Processing Agent is to encoding the biometrics information into a code using an embedded algorithm, and the Iris Image Identification Agent is to compare the attempted code with the code that stored in its database for matching. There are two types of matching in this case. If the biometrics system has confirmed personal information, it is a one-to-one matching. If the biometrics system does not know the personal identification information, it becomes a one-to-many (sometimes one-to-millions of people) identification.

Most mobile and ubiquitous applications, such as mobile face recognition, hospital smartcard-fingerprint system, and hand-writing recognitions, use one-to-one identification. The reason behind it is simple: keep false positives low while having a high specificity rate in the biometrics identification. When biometrics is built on the one-to-many identification, which is very common in public sectors (e.g., when a police officer needs to match identification for suspects), the matching

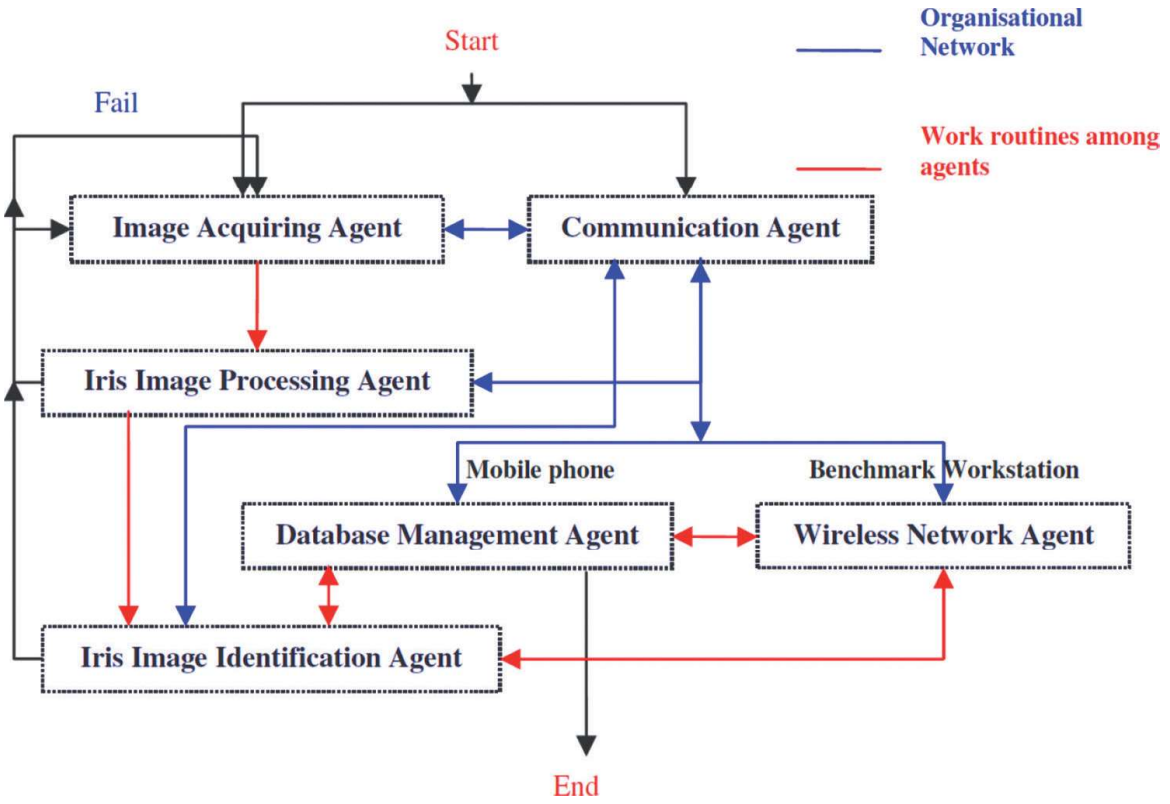

Figure 1.
Distributed agents' organisation network in a typical biometrics system [1].

algorithm and decision threshold become utterly important and need to be customised based on the purpose. A low specificity rate in the biometrics system will lead to a waste of public resources, unfair and biased judgement of individuals.

In this chapter, the author firstly introduces an emerging area of biometrics, namely MedMetrics. The MedMetircs combines medical and biological biometrics with the ultimate aim of identifying patients and their health conditions, drugs, and medical procedures using biometrics codes. To ensure patient data privacy, MedMetrics needs to answer three questions: authentic user, real user, and when to take the action of authorisation. MedMetrics's code is accessible and editable on current events, but all previous information will remain un-editable encryption. It can be used as a fixed baseline blockchain or a time-series blockchain that records temporal codes.

Secondly, this chapter provides insights into MedMetrics in medical science and health care. The author will discuss how traditional biometrics technologies apply to the medical and medical science field, then explain how MedMetrics can revolutionary change the user demographic, shift safety restrictions, define new user applications, and encourage ethical AI regulations in medical science and health care. The novelty of MedMetrics in the areas it applies to, such as the 'MedMetrics Patient Passport' and the 'MedMetrics Drug Passport'. Because the MedMetrics codes are formed based on multiple international standard codes, the introduction of MedMetrics will help ethical and regulatory governance in developing an evaluation of medical biometrics that is trustful and repeatable.

2. MedMetrics in medical science and healthcare

2.1 Recent development in biometrics in healthcare

In the last two decades, biometrics using fingerprints has been accepted and used widely as an identification measure for clinicians in hospital settings. Hospital and healthcare staff can use a smartcard with a user name and password (as a personal signature) and fingerprints for patient data access, test assignment, and drug subscriptions. In the recent 5 years, one encouraging move is that patients started to accept using face recognition on mobile phones to gain healthcare applications. Encrypted face patterns became an acceptable biometric password and inspired several applications. For example, UK residents can now complete the onboarding process for their National Health Service (NHS) login using face recognition via Apple Face ID iProov Genuine Presence Assurance [2]. After the secure facial verification, residents can access essential services online, such as appointments, personal health records, and ordering repeat prescriptions. The Programme Head for NHS login suggested that "More automated tools like this will help us to improve the experience of our users, increase demand capacity and ensure nobody is waiting too long to complete identity verification checks to gain access to their digital healthcare services" [3].

Another application that is emerging is using physiological signs as biometrics. Studies show that electrocardiogram (ECG) signals can be used as a biometrics measure [4–6]. Thanks to the highly individualised nature of the ECG, they are ubiquitous and difficult to counterfeit [7]. However, one of the main challenges in ECG-based biometric development is the lack of large ECG databases.

In this chapter, we propose two novel methods in MedMetrics can play revolution roles in the digital health *Era*. MedMetrics is the medical and healthcare biometrics,

which is an ideal tool in health care and clinical settings to assure the correct genuine presence of patients, instruments, drugs, and procedures. The benefits of using MedMetrics identity verification for healthcare include improving digital access to health services, increasing inclusivity and accessibility, enabling contactless engagement, reducing the time and cost of manual administration, protecting privacy, and making security and usability measurable and personalised.

2.2 MedMetrics patient health passport

The first novel method is the '**MedMetrics Patient Passport**'—a unique patient biometrics identity that can be updated with historical information that remains unchangeable. Clinical investigation of medical procedures is highly regulated with national and regional rules and requirements that must be adhered to by investigators, manufacturers, as well as other parties involved in clinical procedures. In the design of 'MedMetrics Patient Passport'. In a digital 'MedMetrics Patient Passport', patients will each have a unique code that includes basic identification, time-series health condition, test results if available, and medical history, including the medication in use.

The basic patient electronic health record (EHR) includes patient name, national identification, ethical group, date of birth, address, etc. This information is personal information biometrics that is often used for patient check-in at hospitals. The time-series health condition will be recorded in the International Classification of Disease (ICD) code and split by hashing space in between events or clinical visits. The medical device will be recorded under the ISO 14155: Clinical investigation of medical devices for human subjects – Good clinical [8].

To evaluate performance in healthcare with MedMetrics, the Healthcare Effectiveness Data and Information Set (HEDIS) can be used. Over 200 million people worldwide enrolled in plans that report HEDIS results. The HEDIS includes more than 90 measures across 6 domains of care, namely: effectiveness of care, access and availability of care, the experience of care, utilisation and risk-adjusted utilisation, health plan descriptive information, and measures reported using electronic clinical data systems [9].

2.3 MedMetrics drug passport

The second method that MedMetrics can help make a revolution in the digital healthcare *Era* is the '**MedMetrics Drug Passport**'. This passport has information about drug's name, place of birth (batch number), place of issue (manufacturer's name), visiting history (known usage in specific health conditions in the format of ICD code), and the record of rejection of entry (known interaction with other drugs, which is recorded in the Anatomical Therapeutic Chemical code). The Anatomical Therapeutic Chemical (ATC) code is a unique code assigned to medicine according to the organ or system it works on. The ATC and the Defined Daily Dose (DDD) as a measuring unit have become the gold standard for international drug utilisation monitoring and research that is defined and maintained by the World Health Organisation WHO. The ATC and DDD system is an internationally agreed code system that can be used to exchange and compare data on drug use at international, national, or local levels.

This MedMetrics Drug Passport is the ultimate documentation that enables many applications that require privacy, transparency, accuracy, and uniqueness. MedMetrics can help to save people's life by providing alerts in drug interactions. There are several types of drug interactions, the main three types are drug-drug/herbal products, drug-disease, and drug-food/alcohol. Software can help clinicians to

detect drug interactions, but many programs have not been updated with the evolving knowledge of these interactions, and do not take into consideration important factors such as patients of different age groups, nutritious levels or ethical groups [10, 11].

The following are how MedMetrics Drug is used under different interaction scenarios:

1. For the drug-drug/herbal products interaction. MedMetrics can help using existing records in comparing the ATC code for drug checking. A risk alert will be given when a MedMetrics Drug Passport is paired with the DDD code and the existing ATC code in the MedMetrics Patient Passport.

Purpose of applications	**Case studies**	**MedMetrics empowerment**
Medication management	Prescribing	Patient identification
	Clinician-order entry	Clinician identification
	Medication reconciliation	MedMetrics Drug Passport: Dosage comparison from historical records
	Drug-safety alerts	MedMetrics Drug Passport
Documentation	Structured text entry	N/A
	Dictation	N/A
Patient management	Disease management	MedMetrics Patient Passport
	Appointment and testing reminders	N/A
	Care instructions	MedMetrics Patient and Drug Passports
	Result notification	N/A
	Patient behaviour modification	N/A
Quality improvement	Management of patient transfer and transition	MedMetrics Patient passport
	The Healthcare Effectiveness Data and Information Set (HEDIS)	MedMetrics Patient passport
Administrative tools	Billing	N/A
	Referral management	MedMetrics Patient passport
	Risk stratification	MedMetrics Patient and Drug Passports
Communication	Doctor-patient communication	N/A
	Multispecialty or team communication	N/A
	Patient support	MedMetrics Patient and Drug Passports
	Patient or clinician social networking	N/A
Public health reporting	Notifiable disease reporting	MedMetrics Patient passport
	Biosurveillance	MedMetrics Patient passport
	Pharmacosurveillance	MedMetrics Drug passport
Healthcare Industry	Health insurance	MedMetrics Patient passport
	Medical devices	MedMetrics Patient passport and international standards
	Emerging technologies and algorithms	MedMetrics Patient and Drug passports

Table 1.
Categories of substitutable applications, selected examples and MedMetrics [12].

2. For the Drug-condition interaction, the ATC code of the new subscripted drug will pair with the DDD code and the ICD code in the MedMetrics Patient Passport and provide a risk alert, respectively.

3. For people who have an allergy to a specific medication, undertaking drugs with a MedMetrics Drug Passport means their risk of allergy will be reviewed before subscription. Many medicines are branded in different names in the pharmaceutical industry while having similar chemistry comments.

In conclusion, this innovative MedMetrics Drug Passport can help save people's lives, especially for the elderly or the cohort under medication treatment.

2.4 MedMetrics in the digital health era

In 2009, the Journal of New England of Medicine had published a Perspective paper on the health information economy [12]. In this sub-section, I have listed the categories of substitutable applications with selected examples—these examples were chosen to demonstrate how MedMetrics performs in the laboratory, clinical practice, hospital, and home-monitoring environment. Combining these exemplars can form different applications that fit a majority of needs in medical and healthcare environments (**Table 1**).

Another main area that MedMetrics can empower is medical science, pharma industry, and scientific biology research. Medicine is increasingly becoming an interdisciplinary area of medical science, surgical intervention, and an information industry identified by governments, healthcare service providers, health product industry, and patients [13]. In **Table 2**, the author summarised how MedMetrics can contribute to medical science in research, safety, and information transfer.

As shown in **Tables 1** and **2**, among the purpose of applications, MedMetrics plays a critical role in authorisation, security, and policymaking.

Purpose of applications	Case studies	MedMetrics empowerment
Medical Research	Clinical trial eligibility	MedMetrics Patient passport and international standard
	Cohort study tools	International standards
	Electronic data capture for trials	International standards
	Laboratory-test interpretation	International standards
	Genomics	International standards
	Guideline management	International standards
Data acquisition	Laboratory data feed	
	Dispensed medication feed	Blockchain, MedMetrics Patient and Drug passport
	Personally controlled health record data feed	Blockchain and MedMetrics Patient
	Public health data feeds (e.g., local context for infectious diseases)	Blockchain, MedMetrics Patient and Drug passport

Table 2.
MedMetrics in medical science: Research, safety and information transfer [12].

3. MedMetrics, artificial intelligence, blockchain and beyond

The data structure in the healthcare system is highly correlated and complex. Many vendors provide healthcare solutions that are IT-centered instead of patient-centered. Thanks to the nature of the data structure in the MedMetrics Passports for patients and drugs, AI, Cloud service, Internet of Things (IoT), and blockchain methods will be able to play a significant role in the upcoming digital health revolution. In this section, the author will introduce how MedMetrics will work in EHR, fuse with AI, blockchain, and IoT (e.g., wearable sensors).

3.1 MedMetrics in electronic health records

Biometric technologies can offer fast and multiple ways of authentication. The encoding and decoding technology have to apply to information that is generated based on the characteristics of objects. Securing electronic health records could become a complex and costly activity, especially in a scenario where multiple actors potentially maintain information [14, 15].

Remote patient monitoring applications mainly focus on connecting clinicians and patients in hospital, community, and home environments. The ultimate goal is to empower both patients and clinicians with timely information for making necessary interventions at an optimised point of service—it will improve the clinical outcome and reduce the risk of burden on the health economics in the long term.

The European Committee for Standardisation has released a set of information security standards to provide a framework for secures to rage and release of health data [16]. The European standards recognise four global security needs that any health information system should accomplish. They are availability, confidentiality, integrity, and accountability [16].

1. Availability is the main barrier between different hospitals and clinics. The MedMetrics Patient Health Passport, blockchain technology will allow health care providers and governing bodies to re-visit the barrier in patient information availability and consider it an integrated solution.

2. Confidentiality of patient information is a major concern for patient EHR storage and sharing. One way to deal with it is that users with the right to access patient information need to be authorised and allowed to do so in order to perform their duties. In this case, the principle of need-to-know is the key concept to be applied [17]. The other way is to unlock the information that is required for a specific purpose, instead of at the same level. In any case, the information accessed should be relevant but also sufficient to provide health care services [18]. Having an encrypted MedMetrics code can dilute the concern of fraud but cannot entirely remove the concern of restricting the users.

3. Integrity is a blade with both sides. A correctly integrated EHR will help clinicians understand patients' health history with a higher likelihood of making correct clinical interventions. However, a merged patient EHR with a fragment of mixed correct and incorrect will bring uncertainty untold and unseen until the data transformation is done. This can be due to human error from the raw record, but the most challenging part is combining complex historical data among different IT platforms and data structures. The MedMetrics deployed

international standards and codes, removing the integrity concern from its root. However, transferring historical data into MedMetrics is yet challenging.

4. Accountability in ethics and governance is equated with answerability, blameworthiness, liability, and the expectation of account-giving [19]. Accountability is central to the discussion in governance for services in public sectors, nonprofit and private, and individual contexts [20, 21]. The MedMetrics passports for patients and drugs are a secure and comprehensive solution to help deal with the privacy and trustfulness issues in the EHR.

The questions of need-to-know, who-to-know, when-to-know, where-to-know are all driven by the relevance of the acceded information. Defining the correct balance between security requirements and the availability of information is a critical goal in a complex healthcare environment [22]. Relevancy is an ambiguous concept that depends on the context. Having a Medimetrics and biometrics authentication of users makes it possible to guarantee that information is accessed, added, and un-modified by the authorised party.

The figure below demonstrates the principle of MedMetrics and how it might work in the healthcare system (**Figure 2**).

3.2 MedMetrics and artificial intelligence

This sub-section will introduce how AI and blockchain can seamlessly work with the MedMetrics infrastructure. Clinical decision-making support uses AI algorithms to support clinicians, healthcare providers, and insurance companies to make real-time clinical or operational decisions. Some companies have implanted AI in the healthcare pipeline. For example, Sensyne Health is the UK's first public listed company in clinical AI, partnered with Oxford University Hospitals and the University of Oxford. It provides AI solutions to both life sciences challenges and healthcare solutions. Another example is Nuance, a company that partnered with Microsoft to provide Healthcare AI solutions and services.

3.2.1 Natural language processing models

MedMetrics is a group of healthcare codes that reflect the uniqueness of patient and drug information. The data structure means it is suitable for natural language processing (NLP) models such as the Bert model [23], a pre-training of deep

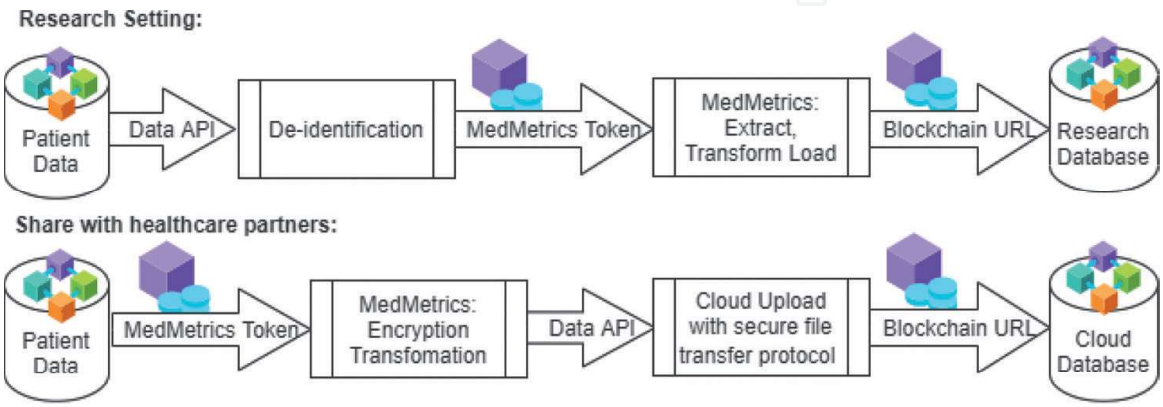

Figure 2.
MedMetrics data pipeline in healthcare.

bidirectional transformers for language understanding. Several Bert models were designed for ICD code. For example, Med-Bert is a method that uses pre-trained contextualised embedding on large-scale structured electronic health records for disease prediction [24]. BEHRT is a deep neural sequence transduction model for EHR that simultaneously predicts the likelihood of 301 conditions in one's future visits [25]. Med-BERT used ICD-9 and ICD-10 codes for diagnosis and the BEHRT used the Clinical Practice Research Datalink (CPRD). The CPRD contains longitudinal primary care covering 35 million patients in the UK. Both Med-BERT and BEHRT proved to be a powerful tools in transferring reactive treatment into preventive medicine at the national level.

3.2.2 Federate learning models

Federated learning is a learning paradigm seeking to address the problem of data governance and privacy by training algorithms collaboratively without exchanging the data itself [26]. Given that scores of data are widely spread across hospitals/individuals, a decentralised computationally scalable methodology is needed [27].

The combination of MedMetrics and Federate Learning will benefit disease prediction studies with small local training datasets, reduce data collection expenses, and accelerate the pace of artificial intelligence-aided healthcare. It will help deal with multi-arm clinical studies across different counties (hence have different data privacy policies) and develop predictive models that require data feeding from time to time.

3.2.3 AI in physiological sensor data

Body Sensor Network (BSN) [28] is one of the most exciting concepts in patient home monitoring. It builds a continuous information hub that can provide real-time and long-distance monitoring. The usage of BSN is still a relatively new area in biometrics. There is a great potential for using one or multiple BSN for personnel identification in healthcare settings.

One of the most mature areas in physiological sensor data biometrics is ECG biometrics. ECG has emerged as a biometrics method with promising results. But same as other sensor technologies, the measurement signals come with sensor failures and measurement variance. On an individual basis, ECG signals can be influenced by physical and psychological changes, such as emotional and mental states, exercise, body position, diets, physical diseases, and positions of electrodes [5]. In addition, signal-acquisition devices produce noises such as from power line interference, baseline wandering, and electrode motion artefacts [29]. Therefore, future work in ECG biometric algorithms is still needed to deal with the concurrence of noises and sample variation.

In applications using ECG as biometrics measures, technologies such as convolutional neural network (CNN), recurrent neural network (RNN), graph regularised non-negative matrix factorisation and sparse representation, One-Dimensional Multi-Resolution Local Binary Patterns, and multi-feature collective non-negative matrix factorisation have been used for pattern recognition (**Figure 3**) [30–35].

3.3 MedMetrics and blockchain

Telemedicine, telehealth, EHR systems, automated retrieval, or update of the electronically stored patient data are common issues that restrict data sharing in the medical science and healthcare sector. Blockchain is a technology in data encryption/

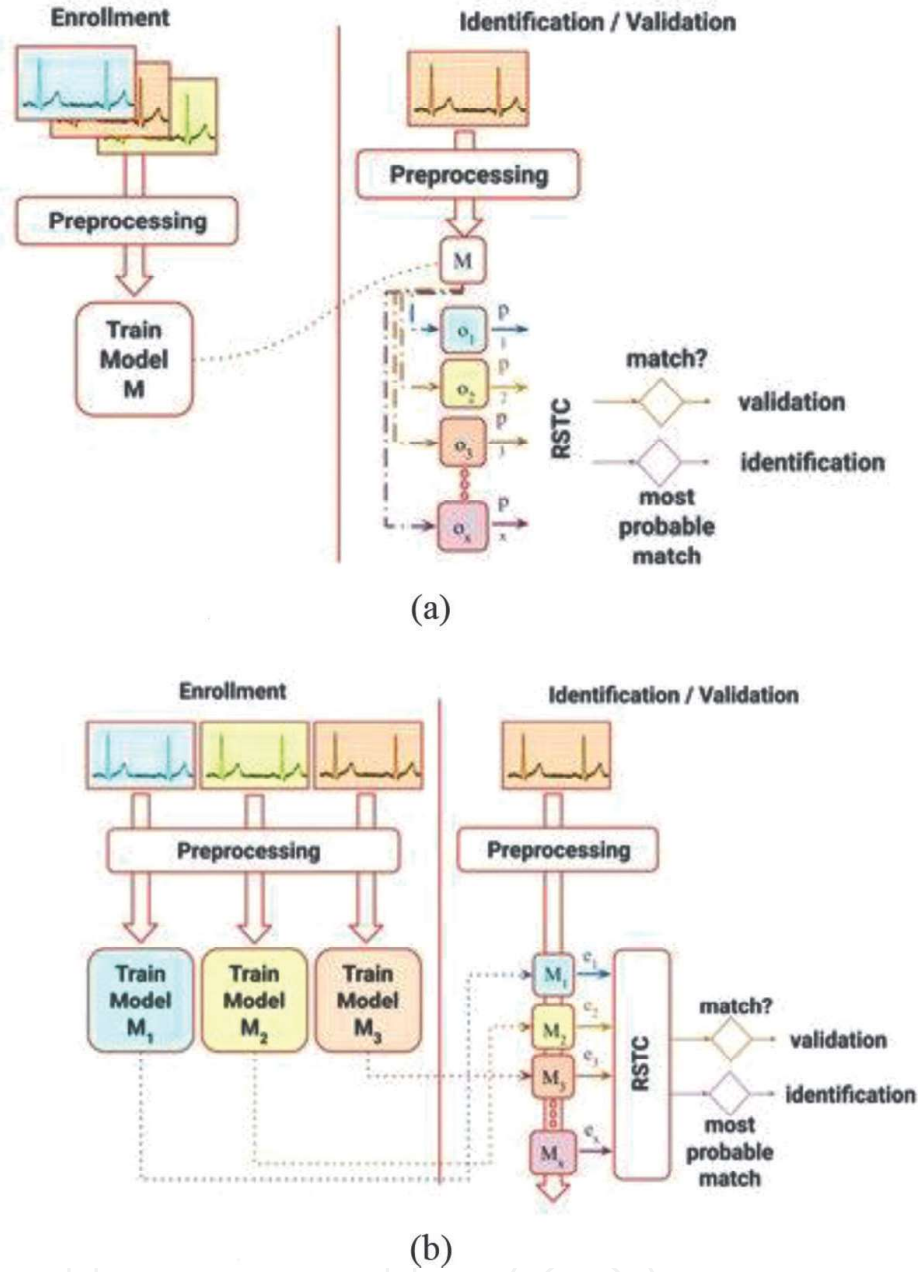

Figure 3.
Examples of deep learning infrastructure for ECG authorisation. (a) an example of a CNN infrastructure, (b) an example of an RNN infrastructure [35].

decryption and tracking. It accelerates innovation, enhances trust, and improves efficiency by overcoming data openness, transparency, and trust concerns. Research suggested that the blockchain might transform how decisions and the interactions between clinicians and patients are recorded [36]. Digital medicine is a field concerned with the use of technologies as tools for measurement and intervention in the service of human health [37]. In the digital medicine environment, blockchain technology will provide AI-based algorithms and applications with the guardian of privacy and authenticity [38].

Due to the size of ever-growing patient data and the future-proof institutional and nationwide service infrastructure, technology developers and health service providers gradually moved towards cloud service. The advancement in cloud networks has enabled connectivity of both traditional networked elements and new

devices from IoT [39]. The governance and standard in supporting Cloud service are ready in taking on new healthcare applications. For the Cloud Service, Health Level Seven International (HL7) framework is a globally accepted standard. HL7 is the global authority on standards for interoperability of health technology with members in over 55 countries [40]. Moreover, the Fast Healthcare Interoperability Resources (FHIR) is a standards framework created by HL7 that combines HL7, CDA product lines and web standards.

By using MedMetrics and blockchain, the internationally identifiable MedMetrics code will provide a seamless solution to make patient data transferable, traceable, and interoperable between hospitals and different countries.

4. Conclusion

Clinical science and medical research in healthcare is an evidence-based practice. The three main pillars for the next generation of digital health and the medical information revolution are securely encrypted data (e.g. using blockchain), artificial intelligence, and governance standard and regulations. The information governance, patient health and safety, ethics and fairness, and economic cost all suggest that a more internationally agreed and unified measure is required to support the upcoming digital health revolution.

Biometrics technologies have been broadly used in the public sectors, including the army, door entry, and data access systems, in authorising personnel access and data access for employees. However, in the healthcare sector, biometrics technologies are mainly used by doctors to access patient information (using user names and fingerprints for one-to-one authorisation). There is an emerging trend of using face recognition to log into online health services, but it is more to combine with mobile authorisation, such as Apple face recognition plug-in, instead of healthcare provider.

The slow movement of using biometrics in the health and care sectors is mainly due to the lack of regulation and policy support for patient data protection. There are hundreds of applications available in the commercial market to suggest they can provide healthcare biometrics solutions in hospitals, doctor's offices, and patient's mobile devices for patient data access control. However, the path of transferring patient EHR among devices, platforms, and hospitals is unclear at the law and regulation level. Due to this reason, most biometrics applications are based on individual hospitals, certain medical procedures, or specific clinics. The legal developments in healthcare have been driven by the public concern for personal privacy and confidentiality.

The MedMetrics passports for patients and drugs will help enable and scale up the innovation in the digital health industry. The MedMetrics Drug Passport can avoid preventable medical procedure mistakes, such as giving the wrong medication. By combining with the blockchain, the MedMetrics Patient Passport can provide a secure healthcare data storage and transfer infrastructure.

Beyond the novel solution in dealing with data privacy, the MedMetrics Patient and Drug Passports will help prevent fraud. The technical challenge of these paradigm shifts is interoperability for supporting the delivery of care at multiple locations by multiple carers who need to share the patient health record [41]. By applying AI algorithms, MedMetrics can identify patients with different health conditions as recorded in the previous record. This will help to prevent fraud in health insurance. By combing an AI layer, the MedMetrics can also alert clinicians when the newly collected MedMetrics information is largely different from the previous record, which

means that patient may need a medical review. The concept of MedMetrics and its deployment will change the user demographic of healthcare applications that healthcare providers would fuse into their clinical practice based on the current healthcare regulations. The developments in standardisation within digital health will help lower long-term costs in public health and improve the quality of healthcare.

In conclusion, biometrics in medical science is an emerging area. The benefits of using biometric identity verification for healthcare are increasing thanks to emerging technologies in blockchain, IoT, fast-speed mobile networks, and more and more powerful mobile phone devices. However, safely implementing biometrics technologies in applications, especially in healthcare and medical settings, is still more prominent in response to a government-led, regulation-based infrastructure. The concept of MedMetrics can change the user demographic, shift safety restrictions, define new user applications, and encourage ethical AI regulations in medical science and health care. It will boost the next generation of biometrics in medical science and health care and encourage hospital-centered, patient-centered, or service-catered applications.

Acknowledgements

The author thanks Prof. David Clifton for mentoring and supporting her in the Daphne Jackson and Royal Academy of Engineering Career re-entry Fellowship. The author thanks Prof. Chris Chatwin, Dr. Rupert Young, Department of Engineering and Design, University of Sussex, United Kingdom, for their supervision in my D.Phil study on mobile iris biometrics.

This work was supported by the Royal Academy of Engineering, Daphne Jackson Trust, Oxford John Fell Fund (0011028), Wellcome Trust (217650/Z/19/Z) for their funding support.

Conflict of interest

The author declares no conflict of interest.

Author details

Huiqi Yvonne Lu
Department of Engineering Science, Institute of Biomedical Engineering, University of Oxford, United Kingdom

*Address all correspondence to: yvonne.lu@eng.ox.ac.uk

References

[1] Lu H, Chatwin CR, Young RC. Iris recognition on low computational power mobile devices. In: Biometrics-Unique and Diverse Applications in Nature, Science, and Technology. London: InTechOpen; 2011. p. 2

[2] Bud A. Facing the future: The impact of apple FaceID. Biometric Technology Today. 2018;**2018**(1):5-7

[3] Available from: https://www.iproov.com/what-we-do/industries/healthcare [Accessed: 06 Jan 2022]

[4] Odinaka I et al. ECG biometrics: A robust short-time frequency analysis. In: 2010 IEEE International Workshop on Information Forensics and Security. London: IEEE; 2010. pp. 1-6

[5] Pinto JR, Cardoso JS, Lourenço A. Evolution, current challenges, and future possibilities in ECG biometrics. IEEE Access. 2018;**6**:34746-34776

[6] Pouryayevali S, Wahabi S, Hari S, Hatzinakos D. On establishing evaluation standards for ECG biometrics. In: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). London: IEEE; 2014. pp. 3774-3778

[7] Ingale M, Cordeiro R, Thentu S, Park Y, Karimian N. ECG biometric authentication: A comparative analysis. IEEE Access. 2020;**8**:117853-117866. DOI: 10.1109/ACCESS.2020.3004464

[8] ISO 14155:2020. Clinical Investigation of Medical Devices for Human Subjects—Good Clinical Practice. Geneva, Switzerland: IOF Standardization, ISO; 2020

[9] HEDIS and Performance Measurement', National Committee for Quality Assurance. Available from: https://www.ncqa.org/hedis/ [Accessed: 06 Jan 2022]

[10] Mallet L, Spinewine A, Huang A. The challenge of managing drug interactions in elderly people. The Lancet. 2007; **370**(9582):185-191. DOI: 10.1016/S0140-6736(07)61092-7

[11] Hitchings AW. Monitoring drug therapy. Medicine. 2016;**44**(7):427-432. DOI: 10.1016/j.mpmed.2016.04.004

[12] Mandl KD, Kohane IS. No small change for the health information economy. The New England Journal of Medicine. 2009;**360**(13):1278-1281. DOI: 10.1056/nejmp0900411

[13] I. National Research Council Committee on Engaging the Computer Science Research Community in Health Care. The National Academies Collection: Reports funded by National Institutes of Health. In: Stead WW, Lin HS, editors. Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions. Washington (DC): National Academies Press (US); 2009 Copyright ©, National Academy of Sciences, 2009

[14] Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. International Journal of Medical Informatics. 2007;**76**(5-6):471-479

[15] Flores Zuniga AE, Win KT, Susilo W. Biometrics for electronic health records. Journal of Medical Systems. 2010;**34**(5):975-983. DOI: 10.1007/s10916-009-9313-6

[16] Klein GO. Health informatics—Security for healthcare communication,

E. C. F. Standardization. Methods of Information in Medicine. 2002;**41**(4): 261-270

[17] Blobel B. Authorisation and access control for electronic health record systems. International Journal of Medical Informatics. 2004;**73**(3):251-257

[18] van der Linden H, Kalra D, Hasman A, Talmon J. Inter-organizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics. 2009;**78**(3):141-160

[19] Dykstra CA. The quest for responsibility. American Political Science Review. 1939;**33**(1):1-25

[20] Shahib HM. Towards Local Government's Integrated Accountability Framework. In: Towards the Local Government's Integrated Accountability Framework. Berlin/Heidelberg, Germany: Springer; 2021. pp. 115-131

[21] Srivastava V, Mahara T, Yadav P. An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks. International Journal of Cognitive Computing in Engineering. 2021;**2**:171-179

[22] Blobel B. Application of the component paradigm for analysis and design of advanced health system architectures. International Journal of Medical Informatics. 2000;**60**(3):281-301

[23] Devlin J, Chang M-W, Lee K, Toutanova K. Bert: Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of NAACL-HLT. 2019. pp. 4171-4186

[24] Rasmy L, Xiang Y, Xie Z, Tao C, Zhi D. Med-BERT: pretrained contextualized embeddings on large-scale structured electronic health records for disease prediction. NPJ Digital Medicine. 2021;**4**(1):1-13. DOI: 10.1038/s41746-021-00455-y

[25] Li Y et al. BEHRT: Transformer for electronic health records. Scientific Reports. 2020;**10**(1):1-12

[26] Rieke N et al. The future of digital health with federated learning. NPJ Digital Medicine. 2020;**3**(1):1-7. DOI: 10.1038/s41746-020-00323-1

[27] Brisimi TS, Chen R, Mela T, Olshevsky A, Paschalidis IC, Shi W. Federated learning of predictive models from federated electronic health records. International Journal of Medical Informatics. 2018;**112**:59-67. DOI: 10.1016/j.ijmedinf.2018.01.007

[28] Lo BP, Thiemjarus S, King R, Yang G-Z. Body Sensor Network—A Wireless Sensor Platform for Pervasive Healthcare Monitoring. London: IEEE; 2005

[29] Limaye H, Deshmukh V. ECG noise sources and various noise removal techniques: A survey. International Journal of Application or Innovation in Engineering & Management. 2016;**5**(2): 86-92

[30] Donida Labati R, Muñoz E, Piuri V, Sassi R, Scotti F. Deep-ECG: Convolutional Neural Networks for ECG biometric recognition, Pattern Recognition Letters. Vol. 126. 2019. pp. 78-85. DOI: 10.1016/j.patrec.2018.03.028

[31] Louis W, Komeili M, Hatzinakos D. Continuous authentication using one-dimensional multi-resolution local binary patterns (1DMRLBP) in ECG biometrics. IEEE Transactions on Information Forensics and Security. 2016;**11**(12):2818-2832. DOI: 10.1109/TIFS.2016.2599270

[32] Li R, Yang G, Wang K, Huang Y, Yuan F, Yin Y. Robust ECG biometrics using GNMF and sparse representation.

Pattern Recognition Letters. 2020;**129**:70-76. DOI: 10.1016/j.patrec.2019.11.005

[33] Ibtehaz N et al. EDITH: ECG biometrics aided by deep learning for reliable individual authentication. IEEE Transactions on Emerging Topics in Computational Intelligence. 2021;**1**:1-13. DOI: 10.1109/TETCI.2021.3131374

[34] Huang Y, Yang G, Wang K, Liu H, Yin Y. Robust multi-feature collective non-negative matrix factorization for ECG biometrics. Pattern Recognition. 2022;**123**:108376. DOI: 10.1016/j.patcog.2021.108376

[35] Belo D, Bento N, Silva H, Fred A, Gamboa H. ECG biometrics using deep learning and relative score threshold classification. Sensors. 2020;**20**(15):4078. Available from: https://www.mdpi.com/1424-8220/20/15/4078

[36] Leeming G, Ainsworth J, Clifton DA. Blockchain in health care: Hype, trust, and digital health. The Lancet. 2019;**393**(10190):2476-2477

[37] Goldsack JC et al. Verification, analytical validation, and clinical validation (V3): the foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs). npj Digital Medicine. 2020;**3**(1):55. DOI: 10.1038/s41746-020-0260-4

[38] Elenko E, Underwood L, Zohar D. Defining digital medicine. Nature Biotechnology. 2015;**33**(5):456-461

[39] Faizullah S, Khan MA, Alzahrani A, Khan I. Permissioned Blockchain-Based Security for SDN in IoT Cloud Networks. In: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT). London: IEEE; 2020. pp. 1-6. DOI: 10.1109/AECT47998.2020.9194181

[40] Elena Vega D. Automated interoperability testing of healthcare information systems. In: Memon A, editor. Advances in Computers. Vol. 85. Amsterdam, Netherlands: Elsevier; 2012. pp. 213-276

[41] Shoniregun CA, Dube K, Mtenzi F. Laws and standards for secure e-healthcare information. In: Electronic Healthcare Information Security. Berlin, Germany: Springer; 2010. pp. 59-100