DNA Based Cryptography to Improve Usability of Authenticated Access of Electronic Health Records

C. S. Sreeja[1(✉)], Mohammed Misbahuddin[2], and B. S. Bindhumadhava[2]

[1] Christ University, Bangalore 560029, Karnataka, India
sreejasukumaran@gmail.com
[2] Centre for Development of Advanced Computing (C-DAC), Bangalore 560100, Karnataka, India
mdmisbahuddin@gmail.com, bindhu@cdac.in

Abstract. The quality of health care has been drastically improved with the evolution of Internet. Electronic health records play a major role in interoperability and accessibility of patient's data which helps in effective and timely treatment irrespective of the demographic area. The proposed model is to ensure and monitor maternal health during pregnancy and to create awareness alerts (options include messages, voice alerts or flash the system) based on the individual health record. The system aims to prevent maternal death due to medical negligence and helps to make recommendations to prevent future mortality based on medical history and take appropriate action. Authentication is a critical aspect considering the trade-off between usability and security whereas data breach and related cybercrime are major concerns in health care. The proposed model uses DNA based authentication techniques to ensure usability and confidentiality of electronic data, Aadhaar to prevent unauthorized access to patient's data in case of emergency without affecting availability.

Keywords: DNA Cryptography · Confidentiality · Usability · Aadhaar EHR · Data breach · Authentication · M-health

1 Introduction

India as a developing nation health care is also an important domain to be taken care and it needed special care as it involves confidential and sensitive data of patients. Manipulation of health records is always a matter of life and death. Recently death related to medical negligence has become common news, especially during pregnancy and childbirth. This not only affects the citizen's trust in hospitals but also affects the reputation of doctor's community. As per World Health Report ranking India's healthcare system is at 112 out of 190 countries [1, 2]. So, it is high time to implement a proper health care management system to improve the quality of life of citizens and to reduce infant and maternal mortality rate. A proper and systematic medical data recording system based on individual health record will help in reducing the infant

N. Kumar and A. Thakre (Eds.): UBICNET 2017, LNICST 218, pp. 208–219, 2018.
https://doi.org/10.1007/978-3-319-73423-1_19

mortality rate (IMR) and maternal mortality rate (MMR) also helps in minimizing medical malpractices.

The scope of the study includes improving the quality of health care system in India which has key issues like maternal mortality, birth defects etc. by providing an Electronic health record (EHR) and a usable authentication system as the digital data plays a vital role. Digital society is in store for near future for all the countries across the globe and it has a high impact as the online users are increasing day by day. Most of the organizations are globally connected leading to economic growth whereas few domains such as healthcare are not exploiting the online facilities apart from few private hospitals as the data breach and confidentiality issues are major inhibitors.

This paper proposes a simple and usable health care system which concurrently maintains EHR and prevents unauthorized access to it by using DNA based encryption techniques. Aadhaar, 12-digit unique identification number issued by the Unique Identification Authority of India [3] is also incorporated into the proposed EHR and related authentication system as it helps and plays a major role for unique identification of a citizen. The proposed system will be beneficial for m-health based services as the system ensures security without using complex algorithms and the model is Universal and can be implemented in the countries where a unique national ID is used for residents. Linking DNA and EHR has various benefits as the future is of personalized medicine, (e.g. Pharmacogenomics) and real DNA can be used for authentication of EHR. Next section explains the existing EHR systems across the world, merits and demerits, usage of internet connectivity and mobile and its impact on health care.

2 Electronic Health Records Welfare, Challenges and Existing Systems

EHR plays an important role considering the quality of care, patient safety and on time treatment whereas information security issues and data breach related to the health care industry are major concerns. Nir Menachemi and Taleah H Collum gives details on the benefits and drawbacks of EHR systems. In the paper, the authors highlight the potential benefits of EHR and related uses in clinical, organizational and societal and outcomes. EHR systems have many capabilities but main functionalities which improve the quality of health care are Clinical decision support (CDS) tools, Computerized physician order entry (CPOE) systems and Health information exchange (HIE).

All the three criteria mentioned above are of “meaningful use” set forth in the HITECH Act of 2009 [4]. Benefits of using EHR also includes reducing malpractices, increased availability of data which in turn helps in clinical analysis and helps in providing best practices. The major drawbacks for the adoption of EHR are security and privacy concerns whereas financial issues and changes in the workflow are also considered [5].

Most of the countries are shifting towards digitization of data in every field whereas health care is a domain which has more benefits of digitization. Digital health data provides availability and interoperability of health information which is essential during an emergency as it ensures timely treatment and care and helps to reduce mortality. Setting up digital databases will help in HIE at the same time ensuring

security and privacy is a major concern. The majority of the private hospitals are using the benefits of digitization whereas government sectors are still inert to tackle the situation.

The majority of the developed countries have well-defined Health Care System and it varies from nation to nation depending on the economic development and available resources. EHR implementation around the world is reviewed by the author in [6] and gives a quick look of adoption of EHR and related policies across various countries - The United States, The United Kingdom, France including the initiatives by India and claims that the EHR system in India does not have adequate security and privacy. Singapore has one of the most successful health care systems in the world-National Electronic Healthcare Record (NEHR) and has been rated as most efficient in the world by Bloomberg in 2014 [7].

A mobile based application - MOTHER (MObile based maTernal HEalth awaReness is a good initiative developed by Centre for Development of Advanced Computing (C-DAC), India [8]. It is a scheduler for sending customized alerts on maternal and child health related information straightway to the mobile phones of the pregnant and lactating women as voice calls in regional languages. The government of India has taken an initiative to define India's Healthcare future by developing an integrated Health Information system – National eHealth Authority (NeHA) proposed by Ministry of Health and Family Welfare. It will also be responsible for enforcing the laws and regulations relating to the privacy and security of the patient's health information and records. Vision of the program is

- To facilitate the integration of multiple health IT systems through health information exchanges.
- To ensure that security, confidentiality, and privacy of patient data.
- To prepare documents relating to architecture, standards, policies and guidelines for e-Health stores, National Health Information Network (NHIN) and HIE [9].

Population from the rural areas will be more benefited by this initiative as it will promote telemedicine and m-health services. But concurrently data security issues persist and there is a need for secure but less complex techniques considering the fact most of the population rely on mobile based systems [10].

Internet usage statistical reports claim India as the second largest online market with 460 million internet users [11] which is a clear demonstration of growing internet usage. Internet penetration rate of India as per 2016 is 34.8% [12]. World Bank measured Indian rural population as 67.25% as per 2015 report [13], which explicitly indicates most of the people lives in rural areas. Digital India campaign was initiated for setting up broadband services in rural India. Considering Internet connectivity and mobile usage in rural area m-health services will be more usable.

Defining a digital health care system which is secure but with less complexity will be efficient and effective considering the usability of the public. Usability and Security always conflicts but in EHR a balance between both are important. Password-based authentication is still prominent and dominant because of easy to use, considering these facts the proposed system is a password-based authentication using DNA cryptography which is easy to use for both patients and doctors. Instead of using complex algorithms, simple but secure algorithms will be more reliable especially if the EHR is accessed

using mobile and here comes the importance of DNA encryption techniques, which provides security based on biocomputations. Next section gives a review on DNA cryptography, basics of DNA, structure, DNA computing and the digital representation of DNA.

3 DNA Cryptography

Data breach and security issues are major drawbacks resisting the adoption of electronic data on health care as most of the organizations are concerned about the security of patient's electronic data. Encryption and Authentication techniques can play a major role in securing EHR but usability and data availability must be considered. DNA based encryption techniques are the recent branch in Cryptography and it's getting wide acceptance due to the vast parallelism and computational complexity. Computational properties of DNA were first introduced in 1994 by Dr. Leonard M. Adleman of the University of South California to solve the complex computational problem of Mathematics [14].

3.1 DNA

DNA is the genetic blueprint of all living cells. In 1869 DNA was first identified by Swiss physician Friedrich Miescher. DNA is a double-stranded helix of nucleotides. A DNA sequence consists of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T, G and C are complementary [15]. Figure 1 represents nitrogenous bases of DNA [16]. Figure 2 depicts the pictorial representation of the helical structure of DNA [17].

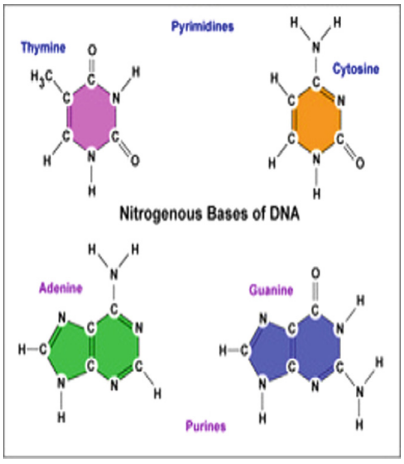

Fig. 1. Nitrogenous bases of DNA

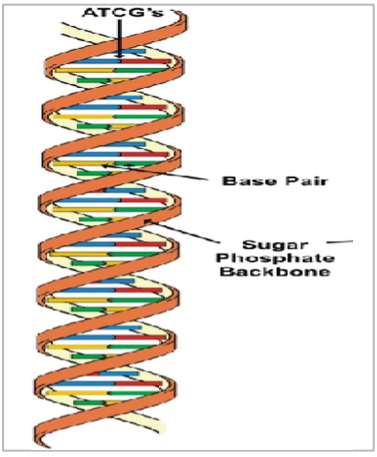

Fig. 2. Helical structure of DNA

3.2 DNA Computing

DNA Computing allows to code A, G, C, T in binary form and this digital representation of the DNA sequences formed the basis of DNA based encryption. Table 1 represents the binary coding of DNA. DNA bases A, G, C and T can be represented as 4! = 24, which adds computational complexity to the sequences if used with biomolecular concepts.

Table 1. Binary representation of DNA bases

A	00
G	01
C	10
T	11

DNA based cryptographic techniques can be used for securing information as it ensures security by means of biocomputations. DNA based encryption methods are widely classified as [18] Symmetric DNA cryptography, Asymmetric DNA cryptography, Pseudo DNA cryptography and DNA Steganography.

Conventional cryptographic techniques used in hybridization with DNA encryption enhances security. DNA based authentication has more applications, especially in EHR. In [18] authors proposed Image and DNA based authentication which ensures usability and security. DNA authentication can be performed using a wet lab or by using digital sequences which are available in the databases in billions. DNA Steganography can be used for transferring confidential medical data especially using Image based Steganography which plays a vital role if medical images are used.

4 Proposed Methodology

The proposed model is to develop an EHR which is a pregnancy registry and tracking system for pregnant women by linking Aadhaar. The purpose of using Aadhaar card is to provide authorized access to patient's data for doctors. The system will have patient's portal where the patient can log in through two-step verification. It also has doctor's portal where registered doctor can login into the database using hospital ID and his own user ID and view patient's health records by using patients Aadhaar. Aadhaar has a QR code which has details of patient embedded in it and can be read by a simple barcode reader or by entering Aadhaar number.

The system aims to protect data as each patient would like to maintain their information privacy. The mother can sign up once pregnancy and estimated due date is confirmed. Based on registered user's EHR and demographic dividend options such as message alerts, voice alerts or flash the system can be used to connect with mothers and share the information related to infant and pregnancy care. The alerts are evoked based on individual's health data and pregnancy stage, emergency numbers can also be shared with expecting moms. Users can rate or raise complaints through the system

after each medical consultation. The information registered will be secured in the centralized database using DNA-based authentication techniques. The centralized database system impacts on reducing IMR and MMR and the mortality due to medical negligence as every act and events are updated in the database and these records also help patients to sue for the medical malpractice.

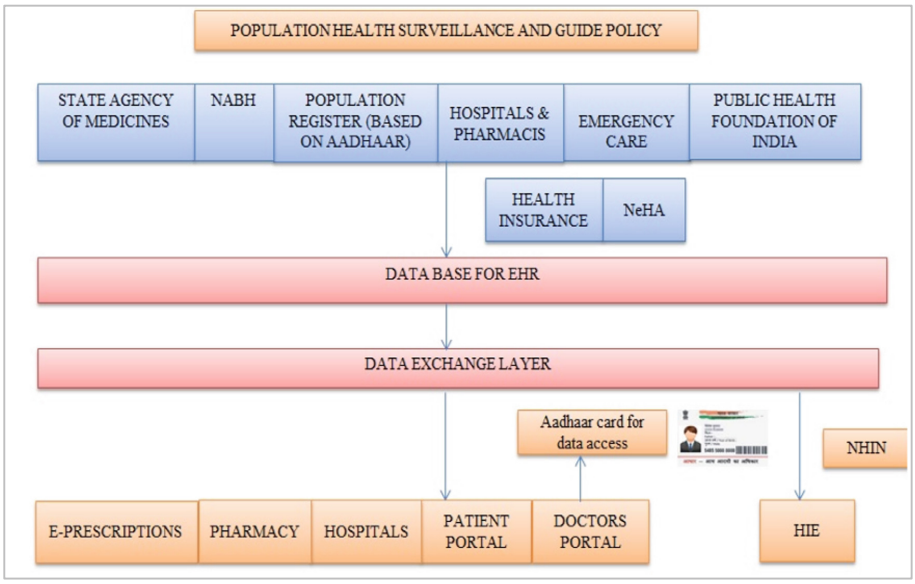

Fig. 3. Proposed architecture for health care system in India

Figure 3 is the architecture proposed for Health Care System in India by including the fields which are essential for the functioning of the centralised database system. It includes National health information network (NHIN), National Accreditation Board for Hospitals & Healthcare Providers (NABH), National health information network (NHIN) and Public health foundation of India. The system can be used for maternal health care and this can be extended for general healthcare in India (Table 2).

Table 2. Notations used in the algorithm

U	User
ID_U	User ID
AID_U	Aadhaar number of ID_U
pwd_{U1}	User selected password during registration
pwd_{U2}	User selected password for security question during registration
AS	Authentication Server
UDS	Unique DNA sequence selected for the user by AS based on AID_U
Pwd_N	New password selected during password change phase

For registration process the patients can take support from Primary health care (PHC) agent or officer and once the registration process is completed the user can view her health record using Aadhaar and OTP received or the details can be shared with the PHC agent to view the health records. If the user wants to view or edit the records the proposed authentication methodology can be used to login and edit the details. Doctors can log in to the EHR portal using his ID and hospital ID and view the patient details using patient Aadhaar number, these will help in case of emergency to access the EHR. The proposed authentication model has three phases – Registration phase, Authentication Phase and password change phase.

4.1 Registration Phase

R1: In the interface or EHR portal two options will be available for Registration.

a. Register as a Patient Login. b. Register as a Doctor's Login
User, Mother can register as a patient by entering essential credentials including AID_U.

R2: AS allows the user to select a valid ID_U and pwd_U.
R3: AS allows the user to select a security question and user can set an answer of her choice.
R4: AS picks a DNA sequence (UDS) depending on user credentials and AID_U. This act as a key factor in DNA Cryptography during user authentication phase.
R5: Registration Phase completed Successfully. An EHR is created for the user, U.
Figure 4 depicts the registration process.

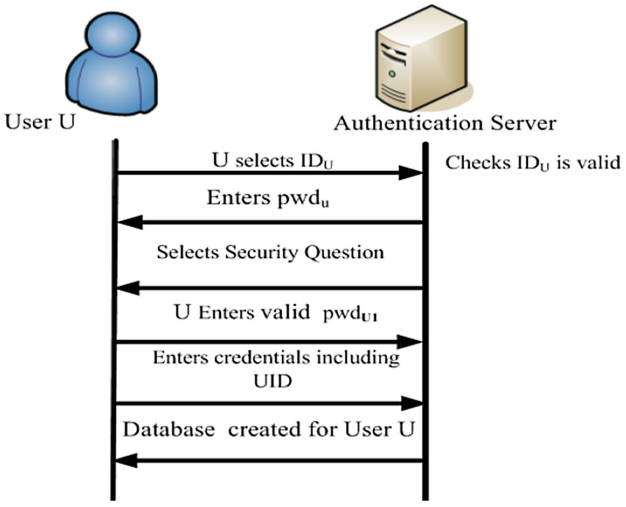

Fig. 4. Registration phase

4.2 Authentication Phase/Login Phase

The proposed authentication phase is a simple, secure and usable technique. This method is a two-step verification phase, but only password based verification is included to ensure usability.

A1: Interface has two options.

a. Patient Login b. Doctor's Login, User enters ID $\rightarrow$ ID_U.

A2: U enters password $\rightarrow$ pwd_{U1}.
A3: AS displays the security question.
A4: U enters pwd_{U2}.
A5: AS picks the unique DNA sequence (UDS) and computes a key value based on ID_U, pwd_{U1}, pwd_{U2} and UDS.
A6: Key computation is based on DNA coding and DNA encryption and generates a hash. During authentication AS computes the key value and if it matches the key value computed during registration the server authenticates the user to the corresponding EHR system.

$$\text{Computation of key value} = pwd_{U1\rightarrow}\ \text{binary} \quad (1)$$

$$= pwd_{U2\rightarrow}\ \text{binary} \quad (2)$$

$$= (pwd_{U1}) \oplus (pwd_{U2}) \quad (3)$$

$$\text{Conversion of Eq. (3) to DNA code based on Table 1} \quad (4)$$

$$\text{DNA encryption by Eq. (4) and UDS} \quad (5)$$

Hash of cipher text generated from Eq. (5) is the key value.
A7: AS checks the key value computed for the user, U during the registration phase, if the key value matches, authentication to the system is granted else denied.

Figure 5 represents authentication phase.

4.3 Password Change Phase

In this phase user, can change the passwords and set the new passwords.

P1: User can enter the details on the interface.
P2: After Authentication phase user, can change the password, security question or both can be changed. The users who prefer additional security can also opt for one-time password (OTP) instead of the security question or as an additive layer depending on the usability of the end-user.

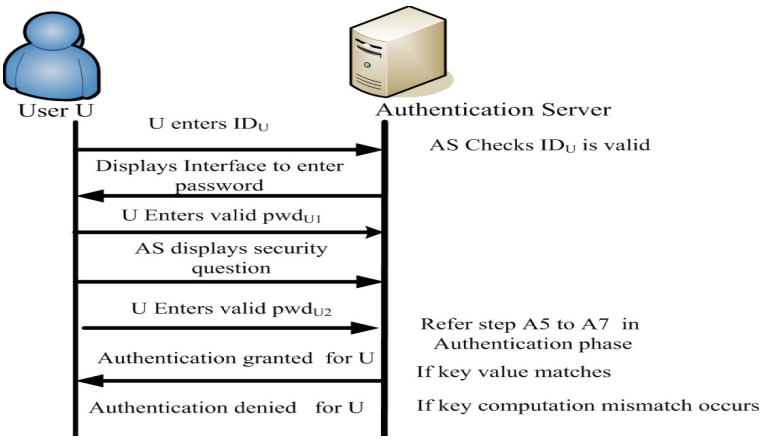

Fig. 5. Authentication phase

5 Security Analysis

The proposed system is simple and usable and can be used by common people without any technical background, considering this fact there is no two-factor verification involved but a two-step password based verification is included for usability. But information security of the system must be maintained for this DNA encryption and hash computations are performed at the server side which ensures security. This section gives security analysis of the proposed system.

5.1 Attack on Password File

The proposed scheme resists password file compromise attack as the password file saved in the database is a computed key value based on hash algorithm as a final output using inputs as:

Binary $((\text{pwd}_{U1}) \oplus (\text{pwd}_{U2})) \rightarrow$ Eq. (1)
DNA Sequence Conversion (Eq. (1)) $\rightarrow$ Eq. (2)
DNA encryption (Eq. (2) and UDS) $\rightarrow$ Eq. (3)

Hash Eq. (3) $\rightarrow$ Eq. (4) $\rightarrow$ output. If the password file is compromised it will be difficult to extract the passwords and enter the system.

5.2 Attack on DNA Sequence

DNA encryption is based on DNA coding, which can be represented as 4! = 24, DNA coding in Table 1 represents one of the digital representation of DNA. The sequence selected by the server will be difficult to guess considering the availability of millions

of DNA sequences in the digital databases and the selection criteria used for DNA reference sequence. It is also possible to generate random sequences, say n which resists the possibility of reference sequence attack.

5.3 Attack on Unique ID

Availability of the Aadhaar or a unique ID of a user to an unauthorized person will not provide access to the EHR. To view the EHR details the knowledge of both passwords are vital. During the registration process users also registers their mobile number for receiving message alerts, voice alerts and to the same number the user receives alert message or notification whenever her EHR is accessed and alerts the valid user about unauthorized attempt to access the data and user can take appropriate action to prevent data access. An option to add OTP ensures additive security and in that scenario, the unauthorized person must have access to all three values.

6 Merits of Aadhaar Usage

Use of Aadhaar in the protocol has potential benefits especially during emergency cases where including the availability of health records and time plays a critical role. If the doctor has the knowledge of patient's Aadhaar he can retrieve the users EHR using his login and hospital login credentials which help in providing effective and timely treatment. Aadhaar will also help in HIE as the unique ID is valid and unique across India. Implementation time of the proposed system can be reduced by using Aadhaar card rather than introducing a new health card system or a smart card for 1.324 billion people, India's huge population.

7 Proof of Concept

This section demonstrates the working of proposed protocol. This section only describes and discusses on the key computation of authentication server for the user U.

Step 1: The user after selecting her valid Id selects the pwd_{U1} as "myehr".
Step 2: AS displays list of security questions, sample question "who is your best friend?" The user enters (pwd_{U2}) as "bob".
Step 3: AS selects a random DNA sequence based on user credentials. DNA sequence selection can be done based on digital sequence, random sequence or from user data. In this study, a sample random sequence of size 300 base pairs (bp) [19] has been generated. Random DNA Sequence generated is:

CTGGTACATTATGTGAACAATGTTCTGAAGAAAATTTGTGAAAGAAGG
ACGGGTCATCGCCTACTATTAGCAACAACGGTCGGCCACACCTTCCATTGT
CGTGGCCACGCTCGGATTACACGGCAGAGGTGCTTGTGTTCCGACAGGCTA
GCATATTATCCTAAGGCGTTACCCCAATCGTTTACCGTCGGATTTGCTATA
GCCCTGAACGCTACATGTACGAAACCATGTTATGTATGCACTAGGTCAACA
ATAGGACATAGCCTTGTAGTTAACACGTAGCCCGGTCGTATAAGTAC

Step 4: Key value computation mainly includes 3 stages

(a) Converting passwords to binary and performing XOR the value generated
1101101011110010110010101101000001000001100010011
01000 → (1), converting (1) into DNA coding based on Table 1.

(b) The value generated is:
TGCCTTACTACCTGAAACAATAGATGAA → (2). A parity bit is added to correct the conversion.

(c) DNA Encryption: The encrypted password which is in DNA form is camouflaged into Random DNA sequence to generate:

CTGGTACATTATGTGAACAATGTTCTGAAGAAAATTTGTGAAA
GAAGGACGGGTCATCGCCTACTATTAGCAACAACGGTCGGCC
ACACCTTCCATTGTCGTGGCCACGCTCGGATTACACGGCAGAG
GTGCTTGTGTTTGCCTTACTACCTGAAACAATAGATGAACCGA
CAGGCTAGCATATTATCCTAAGGCGTTACCCCAATCGTTTACC
GTCGGATTTGCTATAGCCCCTGAACGCTACATGTACGAAACCA
TGTTATGTATGCACTAGGTCAACAATAGGACATAGCCTTGTAG
TTAACACGTAGCCCGGTCGTATAAGTAC →(3),Cipher sequence.

(d) Computing Hash: Hash of the encrypted sequence is computed using SHA-2.
843a81d0051ede0a3a4b1affc7e1a9f3589d91db29048a7059e
74f0a57f11022 → (4)

8 Conclusion and Future Work

In this paper, a methodology has been proposed to reduce the IMR and MMR rate in India which also reduces the medical malpractice related to childbirth and pregnancy as EHR helps to track every records and event. The healthcare system can be integrated for general health care to ensure better treatment. The proposed health care architecture can be integrated for general healthcare system by combining with regulatory agencies for better performance. The work also focuses on the usable authentication of the system by a novel DNA based authentication which uses DNA encryption and unique ID- Aadhaar considering patients usability and data security.

Future work is to propose a single sign-on mechanism for securing electronic health records using Aadhaar by integrating maternity and infant care, health insurance policies, national immunization registry, HIE etc. into a single platform and connect to a centralized database. DNA based authentication techniques can be used with conventional techniques for a secure environment.

References

1. Jayaraman, V.R.: 5 Things to know about India's Healthcare System. http://forbesindia.com/blog/health/5-things-to-know-about-the-indias-healthcare-system/#ixzz3S3WIt74N. Accessed 11 Sept 2014
2. Srinivisan, R.: Health Care in India-Vision 2020, vol. 1. Government of India, Planning Commission of India, New Delhi (2010)
3. What is Aadhar Card – Its Uses, Benefits and Why You Should Have it! http://www.aadharcardkendra.org.in/what-is-aadhar-card-benefits-uses-1424/
4. Blumenthal, D., Tavenner, M.: The meaningful use regulation for electronic health records. N. Engl. J. Med. **363**(6), 501–504 (2010)
5. Menachemi, N., Collum, T.H.: Benefits and drawbacks of electronic health record systems. Risk Manag. Healthc. Policy **4**, 47–55 (2011)
6. Stone, C.P.: A Glimpse at EHR Implementation Around the World: The Lessons the US Can Learn. The Health Institute for E-Health Policy, May 2014
7. Wee, Y.H., Zhou, Y., Tayi, G.K.: IT-enabled healthcare integration: the case of National Electronic Health Records in Singapore. In: PACIS (2015)
8. eIndia 2012 Award to Mother Project. https://cdac.in/index.aspx?id=aboutus_mother_award
9. Concept Note- National eHealth Authority (NeHA). https://www.mygov.in/sites/default/files/master_image/NeHA%20Concept%20Note%20Eng.pdf. Accessed 16 Mar 2015
10. Statistics and facts on Internet Usage in India. https://www.statista.com/topics/2157/internet-usage-in-india/
11. Rural population (% of total population) in India. http://www.tradingeconomics.com/india/rural-population-percent-of-total-population-wb-data.html
12. India internet users. http://www.internetlivestats.com/internet-users/india/
13. The World Bank, Rural population (% of total population). http://data.worldbank.org/indicator/SP.RUR.TOTL.ZS
14. Adleman, L.M.: Molecular computation of solutions to combinatorial problems. Science **266** (5187), 1021–1023 (1994). AAAS-Weekly Paper Edition
15. Sreeja, C.S., Misbahuddin, M., Mohammed Hashim, N.P.: DNA for information security: a survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology. In: International Conference on Computer and Communications Technologies (ICCCT), pp. 1–6, 11–13 December 2014. https://doi.org/10.1109/iccct2.2014.7066757
16. Structure of DNA. http://geneticsk8vaneckv.weebly.com/structures-of-dna.html
17. DNA: Definition, Structure & Discovery. http://www.livescience.com/37247-dna.html
18. Misbahuddin, M., Sreeja, C.S.: A secure image-based authentication scheme employing DNA crypto and steganography. In: Proceedings of the Third International Symposium on Women in Computing and Informatics. ACM (2015). https://doi.org/10.1145/2791405.2791503
19. Random DNA Sequence Genenartor. http://www.faculty.ucr.edu/∼mmaduro/random.htm