

Security of the Health Record Preserving the Privacy of the Patients

Mr. Mbaye Mouhamadou Moustapha¹ and Dr. Gaye Abdourahime²

¹⁻²Department of Computer Engineering and Communication University Alioune DIOP of Bambey, Senegal
Email: m3moustapha@gmail.com, abdourahime.gaye@uadb.edu.sn

Abstract—Electronic Health records offer real benefits in terms of accessing and storing patient health information, which can improve patient care management. However, the attractive features of electronic records (accessibility, portability and portability of patient health information) also present privacy risks. Security concerns stem in part from the origins of health informatics. In the past, organizations protected the identity of subjects by removing identifiers, such as last name, first name, and social security number; however, computer scientists have addressed the privacy of data of various types by showing that Health data can be anonymized to named individuals using simple automated methods. Thus, the objective of this paper is to propose cryptographic solutions that are based on DNA cryptographic encryption structures to provide better resistance to existing and modern attacks. In doing so, we will try to show that data could be shared, managed, and analyzed using practical cryptographic protocols without revealing the content of a particular record. We show that our strategy can counter various attacks. Even if the system is hacked, as long as the encryption hardware is not compromised, no information that is stored will be disclosed.

Index Terms— Health data, information systems security, privacy, cryptographic encryption, Genome, DNA.

I. INTRODUCTION

Every person under the care of a professional, institution, network or other organization involved in prevention and care has the right to privacy and confidentiality of information about him or her. Organizations need to share person-specific Health data without violating the privacy of their subjects (1). In addition, data protection laws further protect the content of patient records. The link between privacy and personal data protection is enshrined in legislation and case law. (30). Our ability to take advantage of the benefits of IT and to manage emerging threats depends on understanding how to protect personal data.

Thus, it should be recognized that there are many publications on the technical, ethical, and legal aspects of security and privacy. Research in the field covers privacy management of Health data preservation in various environments. Failures have unexpectedly spread to remote components in connection with a common network by attack. The concept of using DNA computing in the fields of cryptography is a possible technology that could bring new hope for strong, even unbreakable algorithms (25). A distinction is made between symmetric key cryptography and asymmetric key cryptography (26). The cryptographic method relies on one of the best-known hash functions to guarantee the anonymity of personal information while offering greater resistance to dictionary

attacks, combined with encryption techniques. The following guarantees are offered as part of the cryptographic service: identification and authentication, confidentiality, and integrity. The originality of the method lies in the way the hashing and encryption techniques are combined: as in asymmetric encryption, two keys are used but the private key depends on the identity of the patient [28; 29].

The objective of this paper is to provide knowledge to mitigate privacy threats from their Health records. Thus, the main objective is to encrypt the disease in clear text and hide it as a word composed of letters and numbers. We do not intend to use real DNA to perform the cryptographic process; rather, we will introduce a new method of block symmetric cryptographic algorithm inspired by DNA, which is a new and promising area for information security. It is a combination of classical cryptographic solutions with the advantages of genetic material. Indeed, it is possible to benefit from the advantages of classical cryptographic systems and make them more efficient on certain methods thanks to the use of DNA. There are different ways to use DNA to secure information content. This paper proposes different solutions to use DNA in cryptography.

II. RELATED WORK

An example of such an encryption was proposed by Ayday et al. (13), a privacy-preserving system for storing and processing genomic, clinical, and environmental data using homomorphic encryption and privacy-preserving integer comparison. It is based on homomorphic encryption and its complexity is highly dependent on the number of errors to be tolerated, while allowing Health units to process them in a privacy-preserving manner to perform disease risk testing. This type of encryption is used in many DNA cryptographs (21). This is an encryption scheme where the calculations can be performed on cipher-text and the resulting decryption of cipher-text would be equal to the result of the calculations performed on the plain text. Homomorphic encryption schemes show great promise for use in cloud computing environments as homomorphic encryption allows operations to be applied to encrypted information (3). In contrast to the search and comparison methods of Kantarcioglu et al. Propose to use homomorphic encryption to perform scientific research on integrated genomic data [14].

To ensure better security and reliable data transmission, a new encryption method is proposed here by Paspula et al [12]. The proposed algorithm consists of two rounds that work on the binary values of the message or plaintext. For each round, they secretly select a reference DNA sequence and a secret key (SK). In this algorithm, the binary values or bits are read from the plaintext. A session key, a random number and a DNA sequence are shared over a secure channel between the sender and the receiver before the communication is established. The session key contains information about the key that is used to encrypt the message. The ciphertext is converted to the final ciphertext (S) by using a reference DNA sequence and converting it to a fake DNA sequence called human DNA sequence (S'). Human-made DNA sequence (S'), which makes it difficult for the intruder to extract the original message (23) (22).

There are also several efforts to protect the confidentiality of clinical data, Studies have attempted to promote efficient and accurate reporting of patient safety events, several cryptographic methods have been proposed to solve these problems related to Health data sharing but are still insufficient (15) (16) (17) (18). Other studies show forms of system security, initiatives implemented to improve patient safety. Ad hoc electronic Health record (EHR) systems use cryptographic protocols to securely store Health information and to define access rights for Health units. Narayan, Gagne, and Safavi-Naini [19] and Alshehri, Radziszowski, and Raj [20] propose encrypting EHRs based on the attributes or credentials of healthcare providers.

III. SHARING MATERIALS AND METHODS

A. Electronic Patient Records

The electronic patient record is a secure patient management tool that contains clinical data, care data, appointments and schedules, and test results. It aims to improve the quality of care and the efficiency of the health system. The implementation of the common Health record, which is a computerized document of the same structure for all patients, it is an essential tool for transparency, information sharing, traceability of procedures and efficiency of the care system, as well as for decision-making. The Health record must be able to be presented in forms adapted to the person who consults it. With the Health record, physicians and other authorized health and social service professionals responsible for your care can access the records in any hospital and provide you with better care and more effective follow-up. To do this, we need good Health record protection or encryption of certain diseases or lab tests in the Health record to protect privacy (34;35).

B. Structure of DNA

Deoxyribonucleic acid, or DNA, is a biological macromolecule found in all cells and in many viruses. DNA contains all the genetic information, called the genome, which allows the development, functioning and reproduction of living beings. A nucleotide has one of the following four bases: ATGC. The coded genetic information is located inside the chromosomes and each chromosome contains genes that are responsible for various control functions of the human body as a whole. Thus, with DNA testing, it is possible to measure the level of genetic relationships between individuals. Genes are passed on from generation to generation, genetic comparisons can be made to establish a close degree of relationship between individuals, which is called genetic genealogy. However, after sequencing, the DNA is digitized, and this digital data is subjected to a standard and detailed bioinformatics analysis. Thus, physical precautions are not sufficient to protect privacy and ensure the security of digital data can be easily copied, modified, and shared which raises concerns about privacy and freedoms (3, 24).

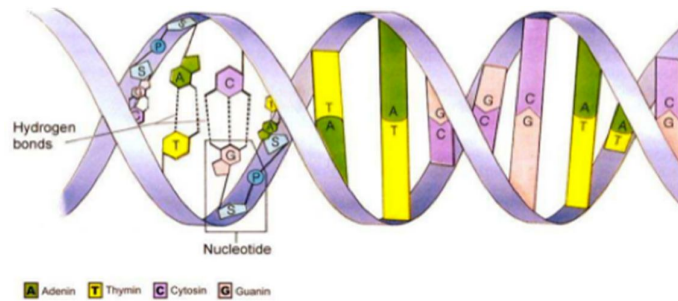


Figure 1: Structure of DNA

C. Cryptography

Alice and Bob have a secret in common that serves as the key for encryption and decryption. These systems are also called secret key encryption because the only key used is the secret shared between the users. Alice must trust Bob and vice versa. This mode of cryptography is the oldest, the most widespread and the most secure. It is nevertheless weakened by the distribution of keys. Indeed, for each couple (Alice, Bob), there must exist a unique key, even for each transmission. The number of keys becomes quickly large which poses the problem of the transmission of the keys by a sure channel.

DNA cryptography encrypts or hides data in terms of DNA sequences. It is a new and broad scientific branch, which includes a variety of fundamental scientific fields: information security (cryptography, shorthand, key management), molecular biology, bioinformatics, biomolecular computation. This can be done using several DNA technologies with biochemical methods. Traditionally, DNA cryptography is implemented using biological tools. This is a new and promising area in information security. It combines classical solutions in cryptography with the strength of genetic material. Molecular calculations can be performed with 25 biological DNA structures and then applied to classical ciphers (31). This DNA cryptographic method can also be interpreted with other schemes to apply this technology in various fields. The performance of DNA cryptography can be tested to prove the effectiveness of an algorithm.

D. Algorithmic Tools

The Health record contains essential and private information about a person's health so that information about the data indicates whether a person is prone to develop a specific type of disease such as AIDS, cancer, diabetes

In these algorithm techniques, we must first define three types of information that allows us to code diseases to better share the data by disclosing the owner of its data but not the secret information of it (32).

Genome-Encode Library Table

First, we need some standard libraries named Genome-Encode Library which includes the uniquely defined 4-bit base sequence for all 256 ASCII characters as shown in Table 1. This Genome-Encode Library is open for anyone to use and encode the Message text in the Genome-Encoded text. It must be encoded in the DNA alphabet. A mapping method is presented where each letter of the English alphabet (A-Y), numbers (0-9) and punctuation marks encoded in 4 DNA letters, such as: B-TCTG or 9 ATGC.

TABLE I: GENOME--ENCODE LIBRARY

TTTT	NUL	TTTC	Space	TTTG	@	TTTA	`	TTCT	Ç	TTCC	á	TTCG	Ł	TTCA	Ó
TTGT	SOH	TTGC	!	TTGG	A	TTGA	À	TTAT	ù	TTAC	ı	TTAG	⌞	TTAA	ß
TCTT	STX	TCTC	"	TCTG	B	TCTA	Ⓑ	TCCT	é	TCCC	ó	TCCG	⌣	TCCA	Ô
TCGT	ETX	TCGC	#	TCGG	C	TCGA	c	TCAT	â	TCAC	ú	TCAG	⌢	TCAA	Ö
TGTT	EOT	TGTC	\$	TGTG	D	TGTA	DEL	TGCT	ä	TGCC	â	TGCG	—	TGCA	ø
TGGT	ENQ	TGGC	%	TGGG	E	TGGA	e	TGAT	å	TGAC	Ń	TGAG	⌣	TGAA	Ø
TATT	ACK	TATC	&	TATG	F	TATA	f	TACT	ä	TACC	*	TACG	ä	TACA	µ
TAGT	BEL	TAGC	'	TAGG	G	TAGA	g	TAAT	ç	TAAC	*	TAAG	Å	TAAA	þ
CTTT	BS	CTTC	(	CTTG	H	CTTA	h	CTCT	ê	CTCC	¿	CTCG	⌢	CTCA	ð
CTGT	TAB	CTGC	)	CTGG	I	CTGA	i	CTAT	ë	CTAC	⌞	CTAG	⌣	CTAA	Ù
CCTT	LF	CCTC	*	CCTG	J	CCTA	j	CCCT	è	CCCC	¬	CCCG	⌢	CCCA	Ú
CCGT	VT	CCGC	+	CCGG	K	CCGA	k	CCAT	ï	CCAC	½	CCAG	⌣	CCAA	Û
CGTT	FF	CGTC	,	CGTG	L	CGTA	l	CGCT	í	CGCC	¼	CGCG	⌢	CGCA	Ý
CGGT	CR	CGGC	-	CGGG	M	CGGA	m	CGAT	ì	CGAC	ı	CGAG	—	CGAA	Ÿ
CATT	SO	CATC	.	CATG	N	CATA	n	CACT	Ä	CACC	«	CACG	⌢	CACA	—
CAGT	SI	CAGC	/	CAGG	O	CAGA	o	CAAT	Å	CAAC	»	CAAG	⌢	CAAA	ˆ
GTTT	DLE	GTTC	0	GTTG	P	GTTA	p	GTCT	Ê	GTCC	⌢	GTCTG	ø	GTC	—
GTGT	DC1	GTGC	1	GTGG	Q	GTGA	q	GTAT	æ	GTAC	⌢	GTAG	⌢	GTA	⌢
GCTT	DC2	GCTC	2	GCTG	R	GCTA	r	GCCT	Æ	GCCC	⌢	GCCG	Ê	GCCA	—
GCGT	DC3	GCGC	3	GCGG	S	GCGA	s	GCAT	ô	GCAC	⌢	GCAG	Ê	GCAA	¼
GGTT	DC4	GGTC	4	GGTG	T	GGTA	t	GGCT	ö	GGCC	⌢	GGCG	Ê	GGCA	Ÿ
GGGT	NAK	GGGC	5	GGGG	U	GGGA	u	GGAT	ö	GGAC	Ä	GGAG	ı	GGAA	§
GATT	SYN	GATC	6	GATG	V	GATA	v	GACT	û	GACC	Ä	GACG	ı	GACA	÷
GAGT	ETB	GAGC	7	GAGG	W	GAGA	w	GAAT	ü	GAAC	Ä	GAAG	ı	GAAA	ˆ
ATTT	CAN	ATTC	8	ATTG	X	ATTA	x	ATCT	ÿ	ATCC	⌢	ATCG	ı	ATCA	°
ATGT	EM	ATGC	9	ATGG	Y	ATGA	y	ATAT	Û	ATAC	⌢	ATAG	⌢	ATA	—
ACTT	SUB	ACTC	:	ACTG	Z	ACTA	z	ACCT	Ü	ACCC	⌢	ACCG	ı	ACCA	ˆ
ACGT	ESC	ACGC	;	ACGG	[	ACGA	{	ACAT	ø	ACAC	Ÿ	ACAG	⌢	ACAA	ˆ
AGTT	FS	AGTC	<	AGTG	\	AGTA		AGCT	£	AGCC	⌢	AGCG	⌢	AGCA	ˆ
AGGT	GS	AGGC	=	AGGG	]	AGGA	}	AGAT	Ø	AGAC	ç	AGAG	ı	AGAA	ˆ
AATT	RS	AATC	>	AATG	^	AATA	~	AACT	×	AACC	Ÿ	AACG	ı	AACA	⌢
AAGT	US	AAGC	?	AAGG	_	AAGA	DEL	AAAT	f	AAAC	Ÿ	AAAG	⌢	AAAA	nbs

Block Coding Table

Also, we need the block encoding table which will be used to replace the existing binary code to the block encoding table. This step is to encode these characters into binary (0,1) based on ASCII encoding. A mapping method is presented where each of the characters is modified into a binary encoded in 4 digits, such as: A-1111 or M-0101. Since all digital information is encoded in binary. This library is not standardized as it can be defined by the user himself.

TABLE II: BLOCK ENCODING TABLE

A : 1111	I : 1011
B : 1110	J : 1101
C : 1100	K : 1010
D : 1000	L : 1001
E : 0000	M : 0101
F : 0111	N : 0100
G : 0011	O : 0110
H : 0001	P : 0010

Base--Binary Library Table

In computer science, in addition to base 10, the binary system (base 2) is used very frequently since Boolean logic is the basis of digital electronics. Two symbols are enough: 0 and 1. This elementary unit which can take only the values 0 and 1 is called a bit. A sequence of eight bits is called a byte. The basic binary library that stores the information on the equivalent conversion of the genomic message padded to a long binary string, i.e., Table II.

TABLE III: BINARY TO DNA CONVERSION TABLE

A	11
C	01
G	10
T	00

E. Cryptography Algorithm

The objective of this proposed algorithm is to provide disease cryptography using DNA which when integrated with existing security methods can increase the reliability and secrecy of data. The most important feature of this algorithm is that it can provide textual data based on the encryption and decryption methodology. Another important feature of this algorithm is that since the data is stored, even if a hacker or intruder gets the data, it will be useless to him (9). In our algorithm we need three types of information: the disease encrypted to convert to DNA in the Genome--Encode library, a block coding table to reduce the starting sequence 4 times smaller during encryption to simplify the transformations, the binary base table to convert a sequence to binary base, and finally the conversion of the binary string to equivalent text (6).

F. Generation of the keys

The key for the encryption and the decryption they are generated randomly by the transmitter and the information on the key is sent to the receiver side via a private channel.

Our algorithm uses a key composed of two parts, its first part is the position P which allows to determine the position in the sequence from which, we removed the nucleotide duplicates.

The second part, the DNA removed by the transmitter R: is the DNA sequence from which we make the extraction of the key.

G. Algorithm

Encryption:

The disease: BONE CANCER

- 1 Using the Genome--Encode library (Tab1), convert the disease into the corresponding DNA sequence, i.e.
TCTGCAGGCATGTGGGTCGGTTGGCATGTCGGTGGGGCTGT
 - 2 We index our sequence to know the position of each nucleotide double.
TC1TG2GG4CA5TG6GG8TC9GG10TT11CA13TG14TC15GG16TG17GG18GC19
 - 3 Generate the decryption key as follows: by choosing four positions in the indexed sequence.
"3.7.12.20" : Location P
"CATGGGTG": nucleotide remove R
 - 4 Then we take the rest of the sequence that we will encrypt
TCTGGGCATGGGTCGGTTCATGTCGGTGGGGC
 - 5 Using the basic binary values (Tab3), convert the sequence to basic binary equivalent.
0001001010100111001010100001101000000111001000011010001010101001
 - 6 Adding bit '1' before and last, we can get this message as follows:
100010010101001110010101000011010000001110010000110100010101010011
 - 7 Finally convert the binary string obtained in the character table to binary-extract (Tab2)
DLMGLMEJEGLEJHMN11
- Send this data in the Health record to the server.

Decryption:

- 1 Download from the server the S
DLMGLMEJEGLEJHMN11
- 2 Since the file is a string and binary, convert the character part in the character table to binary-extract (Tab2)
100010010101001110010101000011010000001110010000110100010101010011
- 3 Then remove '1' from the front and end of the chain:
0001001010100111001010100001101000000111001000011010001010101001
- 4 Using the basic binary values (Tab3), convert the binary to the basic String equivalent
TCTGGGCATGGGTCGGTTCATGTCGGTGGGGC
- 5 Retrieves the decryption key generated at the beginning of the process:

R : "CATGGGTG "

P : "3.7.12.20"

6 Return the removed nucleotides in the starting sequence to their normal position to get the real original sequence:

TCTGCAGGCATGTGGGTCTGGTTGGCATGTCTGGTGGGGCTGT

7 Finally, using the Genome--Encode library (Tab1), convert the DNA sequence to the corresponding letter or number or character in the library.

BONE CANCER

For decryption, as it is a symmetrical key algorithm, the same keys are used but the process is done in the opposite direction to encryption.

IV. PERFORMANCE ASSESSMENT

In this paper, to demonstrate the huge potential and evaluate the statistical performance of the new DNA-based cryptographic key generation algorithm. Where n represents the number of elements in the set and k represents the number of elements selected from the set as the key. The strongest strength of a password deters or prolongs the cracking process. Neither brute force testing nor social engineering techniques can break through in a short time.

$P = \frac{(n + k - 1)!}{k!(n - 1)!}$	n	k	P(kn)
	2	2	253
	2	3	2024
	2	4	12650
	2	5	65780
	2	6	296010
	2	7	1184040

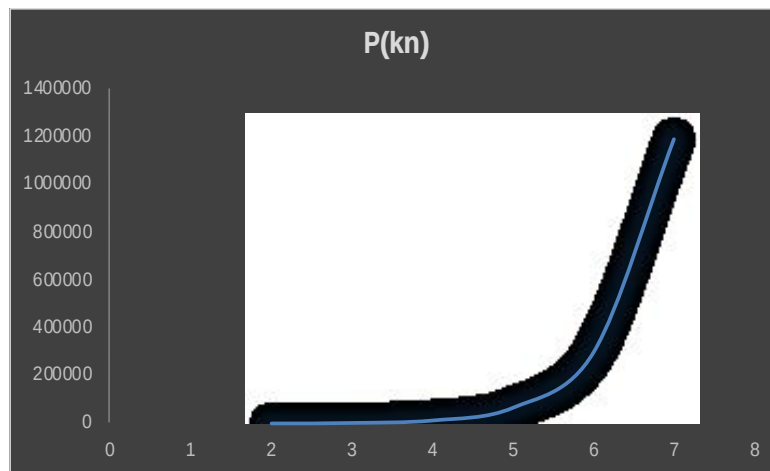


Fig. 2: Ratio of the number of combinations to the size of the key

The analysis of the complexity of an algorithm is important because it reveals its effectiveness for real-time applications. In this work, the computation time of the algorithm was analyzed through experimental tests using functions to measure time. Given a random key obtained from a DNA sequence that is used only once, a cipher text can match any plaintext. Trying all combinations with the key yield's plaintext, all of which have the same probability of representing the original plaintext. Each time the size of the key increases the combinations to find the original text also increases. In the case of a known plaintext, brute force attacks are always useless because

the attacker will not be able to use this information to discover the rest of the key, and since the key changes for each encryption, the previous information is also useless.

V. DISCUSSION

This cryptography has made it possible to develop cryptographic systems based on the use of biological molecules. The idea is that a message can be coded and then drowned in huge amount of information representing DNA and binary codes, to find the desired message, it is enough to have a key that consists of a particular sequence of DNA and the position of pairs of nucleotides. This algorithm is designed in such a way that we randomly select clues in a sequence and their position in a string, which will allow us to randomly draw bases of 2, 4, 6, 8 or more nucleotides in a DNA sequence and their position. The two keys are generated first, and the sequence chosen as the key will be removed from the sequence and the rest of the base sequence is encrypted until we have a binary letter and number code.

For this system to be reliable, there must be no fast algorithm to find the key. Guessing the correct DNA sequence by the attacker is virtually impossible to achieve. The crucial feature of DNA sequences is visibility. Finding secret data in a DNA sequence is difficult because the visibility of sequences is very low. Re-identification is probably the most studied privacy risk in data dissemination and analysis. In such an attack, an unauthorized party examines published Health records that are already under some protection to hide the patient's identity information and attempts to recover the identity of the individuals involved. Such an attack, once successful, can cause serious harm to these patients, such as discrimination and financial losses (2).

Cryptography allows to perform a secure search in an encrypted database, to make statistics on Health records without violating the confidentiality of patients. Encryption is a mini revolution in cryptography and offers many promising industrial perspectives. However, the low efficiency of the existing schemes is still a hindrance for a practical use of these primitives (7). In our algorithm we have tried to make encryption of diseases in the Health record to protect the privacy, this protection system uses two algorithms. The first algorithm is used by the hospital to encrypt the message it wants to protect. The second algorithm is used by the recipient to decrypt the message. Thus, he must introduce the message and the key into the machine to find the original disease.

One can compare this algorithm with the one of indexing by hashing which is carried out via methods of Perceptual Hashing (10). In general, these methods allow identification via the generation of a unique key from a multimedia document. Similar in some respects to cryptographic hashing methods (MD5 algorithm), they differ, however, by the fact that the hash keys corresponding to two documents with a slight difference are relatively close and comparable by methods such as the Hamming distance.

VI. CONCLUSION

Protecting the privacy of a person receiving health care is particularly important. When a person visits a health care professional or is admitted to a health care facility, a record is kept about that person. This record contains personal or Health information about that person. But there are great scientific benefits to the public availability of data: "free and open access to data in medicine has had an extremely positive effect on Health progress. However, data sharing policies must balance scientific benefits with ethical obligations to participants.

At the same time, Health data are integrated into a wide range of applications in various contexts, so privacy and security issues still need to be sufficiently defined and addressed. For example, massive computational capacity is needed to analyze Health data for research purposes, so the cloud is likely to play an important role in managing such data.

REFERENCES

- [1] M. Swan, Blockchain: Blueprint for a new economy, " O'Reilly Media, Inc.", 2015.
- [2] S. Angraal, H. M. Krumholz, W. L. Schulz, Blockchain technology: applications in health care, *Circulation: Cardiovascular quality and outcomes* 10 (9) (2017) e003800.
- [3] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for bioHealth and health care applications, *Journal of the American Health Informatics Association* 24 (6) (2017) 1211–1220.
- [4] C. P. Transaction, M. P. I. MPI, Blockchain: Opportunities for health care, *CP Transaction* (2016).
- [5] C. V. Helliari, L. Crawford, L. Rocca, C. Teodori, M. Veneziani, Permission-less and permissioned blockchain diffusion, *International Journal of Information Management* 54 (2020) 102136.
- [6] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld, Proof of activity: Extending bit-coin's proof of work via proof of stake [extended abstract] y, *ACM SIGMETRICS Performance Evaluation Review* 42 (3) (2014) 34–37.

- [8] T. Zhou, X. Li, H. Zhao, Med-pphis: blockchain-based personal healthcare in-formation system for national physique monitoring and scientific exercise guid-ing, *Journal of Health systems* 43 (9) (2019) 1–23.
- [9] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, X. Zhang, Bbds: Blockchain-based data sharing for electronic Health records in cloud environments, *Information* 8 (2) (2017) 44.
- [10] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, *Journal of Health systems* 42 (8) (2018) 1–18.
- [11] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found health-care intelligence on blockchain with novel privacy risk control, *Journal of Health systems* 40 (10) (2016) 1–8.
- [12] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applica-tions of blockchain technology in medicine and healthcare: Challenges and future perspectives, *Cryptography* 3 (1) (2019) 3.
- [13] C. Esposito, A. De Santis, G. Tortora, H. Chang, K.-K. R. Choo, Blockchain: A panacea for healthcare cloud-based data security and privacy?, *IEEE Cloud Computing* 5 (1) (2018) 31–37.
- [14] W. Liu, S. Zhu, T. Mundie, U. Krieger, Advanced block-chain architecture for e-health systems, in: 2017 IEEE 19th International Conference on e-Health Net-working, Applications and Services (Healthcom), IEEE, 2017, pp. 1–6.
- [15] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for med-
- [16] ical data access and permission management, in: 2016 2nd International Confer-ence on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
- [17] C. Burniske, E. Vaughn, A. Cahana, J. Shelton, How blockchain technology can enhance electronic health record operability, *Ark Invest: New York, NY, USA* (2016).
- [18] V. Buterin, et al., A next-generation smart contract and decentralized application platform, white paper 3 (37) (2014).
- [19] G. Greenspan, Multichain private blockchain-white paper, URL: <http://www.mul-tichain.com/download/MultiChain-White-Paper.pdf> (2015) 57–60.
- [20] M. Aly Konte, Secteur de la santé au sénégal: malaises actuels et perspectives futures; rapport de conférence (2006).
- [21] F. Hane, Production des statistiques sanitaires au sénégal: entre enjeux politiques et jeux d’acteurs, *Santé publique* 29 (6) (2017) 879–886