Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 2306458, 6 pages
https://doi.org/10.1155/2017/2306458

*Review Article*

# A Systematic Review of Security Mechanisms for Big Data in Health and New Alternatives for Hospitals

**Sofiane Hamrioui,[1] Isabel de la Torre Díez,[2] Begonya Garcia-Zapirain,[3] Kashif Saleem,[4] and Joel J. P. C. Rodrigues[5,6,7,8]**

[1]*Bretagne Loire and Nantes Universities, UMR 6164, IETR Polytech Nantes, Nantes, France*
[2]*Department of Signal Theory and Communications, and Telematics Engineering, University of Valladolid, Paseo de Belén 15, 47011 Valladolid, Spain*
[3]*University of Deusto, Avenida de las Universidades 24, 48007 Bilbao, Spain*
[4]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia*
[5]*National Institute of Telecommunications (Inatel), Santa Rita do Sapucaí, MG, Brazil*
[6]*Instituto de Telecomunicações, Lisboa, Portugal*
[7]*University of Fortaleza (UNIFOR), Fortaleza, CE, Brazil*
[8]*University ITMO, St. Petersburg, Russia*

Correspondence should be addressed to Isabel de la Torre Díez; isator@tel.uva.es

Received 21 September 2017; Accepted 30 October 2017; Published 4 December 2017

Academic Editor: Yin Zhang



Computer security is something that brings to mind the greatest developers and companies who wish to protect their data. Major steps forward are being taken via advances made in the security of technology. The main purpose of this paper is to provide a view of different mechanisms and algorithms used to ensure big data security and to theoretically put forward an improvement in the health-based environment using a proposed model as reference. A search was conducted for information from scientific databases as Google Scholar, IEEE Xplore, Science Direct, Web of Science, and Scopus to find information related to security in big data. The search criteria used were *"big data"*, *"health"*, *"cloud"*, and *"security"*, with dates being confined to the period from 2008 to the present time. After analyzing the different solutions, two security alternatives are proposed combining different techniques analyzed in the state of the art, with a view to providing existing information on the big data over cloud with maximum security in different hospitals located in the province of Valladolid, Spain. New mechanisms and algorithms help to create a more secure environment, although it is necessary to continue developing new and better ones to make things increasingly difficult for cybercriminals.

## 1. Introduction

Big data refers to the huge amount of information that is created and proves difficult to analyze in real time, to the extent that traditional databases are not sufficient for dealing with such data [1]. When big data is mentioned, it tends to refer to the three Vs (volume, velocity, and variety) [2], and some even extend this to the five Vs: volume, velocity, variety, veracity, and value [3, 4]. These five characteristics mentioned are defined as follows: volume refers to the size of the data generated, although certain minimums are yet to be established as this is a relative concept. Velocity refers to a large amount of data generated over time. Variety refers to a combination of different information formats, whether structured, semistructured, or without structure. Veracity refers to the fact that none of the data generated is of any use if it is not reliable. Lastly, value refers to the scientific value attributed to this data [5–7].

The term "big data" has been exponentially growing in use since 2011 and is taking on increasing weight in both society and the world of business [8]. As this is a new concept, the lack of trust factor is involved that raises other associated problems [9]. Some of these problems that are seen in the use of big data are rather dangerous. Even though the data is

stored anonymously, there is little control over it, whether this data is private or personal [10]. Moreover, there are benefits in using big data, the most important of which is that it enables the Government to improve quality of life in society via the analysis of vast amounts of information [10].

Traditional databases use standard SQL that generates request and handle relational tables. Owing to the relationships that exist between the tables, utilizing them is not practical because the big data mainly refers to the unstructured information [10]. NoSQL databases have emerged as a result and offer better functionality especially for the purpose of storing and maintaining information on a large scale without being concerned with the format of data in which it is presented. Furthermore, the NoSQL offers high performance for the large volumes of heterogeneous data within a distributed environment [11–15].

Moreover, the terms big data and cloud computing have enormously gained prominence in recent years, and one of the reason for this is because big data is directly related to the cloud [12, 13]. The importance is because the cloud is coming up with the new architecture paradigms in information technology [16–18]. Emerging cloud computing technology offers a solution to reduce the cost of development and operating mobile networks [19–22].

As we have mentioned above, the big data uses cloud and is accessible all around the world from any object with the help of Internet [14]. This raises a big question of security; therefore below a summary of the different levels of big data security over cloud is given. This paper extensively reviews the work carried out by different experts to minimise the risks in utilizing cloud in handling big data [23–26]. Secondly, the concrete solutions are presented to improve the security of big data in a healthcare scenario.

The next section covers the methodology used to obtain and filter the related information required. In Section 3.1, the recent security mechanisms for healthcare big data in cloud are reviewed. Additionally, in Section 3.2 the security model is given and is explained in detail. Lastly, Section 4 provides the conclusion.

## 2. Methods

An exhaustive search was conducted in order to carry out the research of papers on some of the most important and commonly used websites and scientific databases, namely, Google Scholar, IEEE Xplore [27], Scopus [28], Science Direct [29], and Web of Science [30].

A specific search was conducted in each of them using the following words: "cloud" AND/OR "big data" AND "health" AND "security" in the title and abstract. In all cases, the time span was from 2008 to September 2017. Figure 1 shows the 3169 results obtained via the searches conducted, and we also refer to any papers that were disregarded as a result of their being duplicates or having a title that is unrelated to our area of interest. We ended up with 22 papers after having read 134 and seeing which of them proved beneficial to us after viewing the corresponding abstracts.

All the papers related to health. At the end, we decided to use these papers because after reading the others, although initially appearing to cover big data and associated security, we noted that they only mention the big data situation or the situation regarding legislation in Europe and the USA governing data on the cloud.

Therefore, we decided to disregard these as they failed to provide us with relevant information, and in making our selection, we took papers written in English into consideration. After reading the titles and abstract and ending up with the 134 papers mentioned, we then proceeded to read their content and thus determine which of them would provide us with information related to big data and its security on the cloud or on databases it uses to store data.

## 3. Results and Discussion

*3.1. Security Mechanisms Based Literature Review.* In this section, we provide a summary of the main advances made by the scientific community that will help to keep healthcare data more secure. Recently, Wang et al. (2017) enhance attribute-based encryption (ABE) that is introduced by the Cloud Security Alliance (CSA). The improved auxiliary input model based Ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) schemes are presented. While conducting the comparison, the improved model considers also the encryptor leakage (leakage of randomness) in front of other auxiliary input model. Furthermore, an improved strong extractor from the modified Goldreich–Levin theorem is given. The performance comparison is conducted between the other three leakage resilient CP-ABE and the proposed schemes. The author has programmed the CP-ABE scheme in C language and has implemented it on two different types of processors based platforms by using the pairing based cryptography (PBC) library to test the encryption time.

Cho et al. (2016) provide us with architecture based on a double layer for the working environment with big data. These two layers are the prefiltering layer and the postfiltering layer. The first-mentioned is in charge of searching for and eliminating sensitive personal information from the data gathered, which is done in order to make the information anonymous and thus make it more difficult to identify the person in particular. The second, postfiltering layer, disguises the summarized sensitive information following big data analysis [31].

Liu et al. (2015) define a series of steps in which the validity of the data stored is verified externally. External verification is as important as the security provided by the server and, as this is an external agent, certain steps need to be established to maintain data security [32].

Fabiano et al. (2015), from the University of Wyoming, have been developing a variant of the MapReduce paradigm to be applied in security which complies with HIPAA, as well as using the OpenSSL encryption package. To ensure maximum scalability, they implemented a hybrid of the OpenMP-MPL programming paradigm, by means of which they enabled each processing core to be assigned a number of files and then for each core to subdivide these files, depending on the number of threads being used [33].

Yan et al. (2016) propose two security schemes in which the aim is to protect the confidential information of

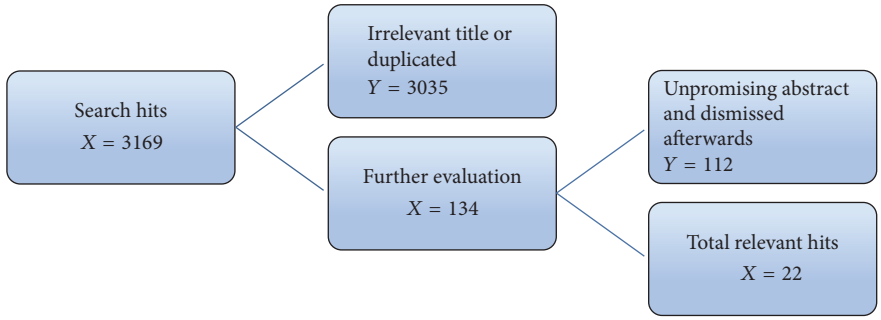


Figure 1: Flow chart of the steps followed in the review.

trusted suppliers. The first scheme focuses on computational efficiency while the second provides better protection at the expense of computational cost. They use proxy-based additive homomorphism with reencryption to design these two schemes for Privacy-Preserving Trust Evaluation (PPTE) [34].

Zhou et al. (2015) propose an encryption algorithm that focuses on image security. This algorithm is based on the Chaos stochastic process and the Line Map principle and is designed to ensure that if an image is encrypted, nothing will continue to be seen if an attempt is made to decrypt the key. The disadvantage of this algorithm is that it can only be used for those images that have the same width and length, although the authors have carried out tests and reached the conclusion that it is a robust algorithm [35].

Hsu et al. (2014) show us how to develop a protocol for the secure transfer of data and also propose a protocol for the transfer of a group key. To do so, they create a variant of the Diffie Hellman algorithm which is designed for one-to-one communication rather than between several individuals. The motivation behind this protocol is to preserve the key refresh, its confidentiality, and its authentication [36].

Jing (2014) comments on the growing use of the cloud as a storage space. To improve security, they propose a double encryption data system, which consists of an initial encryption using the AES encryption algorithm and therefore a symmetric algorithm. They then use the RSA algorithm as an asymmetric algorithm, by means of which two keys are generated—the public and private one. Users are in possession of the private one and use it to decrypt information, thus ensuring that they alone are able to obtain the data in question [18].

Hingwe and Bhanu (2014) explain a database model on the cloud with architecture consisting of two additional layers, which are used depending on whether the data is sensitive or otherwise. Data encryption is added to the layers, and this takes the form of double encryption if the information is deemed sensitive. A key is needed for this encryption and a symmetric key provided by the database server is used for such purpose. Where sensitive information is concerned and hence two layers are used, this is split into two by an algorithm to improve it [37].

Cheng et al. (2014) provide a summary of the most direct threats to which a customer of a cloud supplier may be exposed. Among these threats, the suppliers themselves may use their data for their own interests or cybercriminals may acquire the data, and they propose a simple scheme to deal with these threats involving splitting the data into fragments. After performing a hash function, these fragments are then packaged—what makes this scheme work is that these packages are randomly distributed among different storage points in such a way that they possess no useful information on their own [16].

Thilakanathan et al. (2014) provide us with a security model to be used in monitoring patients via remote devices such as mobile phones and bracelets. This model makes use of double encryption, symmetric encryption, and encryption using the ElGamal algorithm, whereby mobile devices generate the patient's data and this data is encrypted using a symmetric key. The second encryption, which is asymmetric, is used to improve security, and its function will be to encrypt the public key being used.

The disadvantage of using a symmetric key, however, is that it loses the identity of the data [39]. Subashini and Kavitha (2011) explain a security model that does not prevent the database from being hacked but rather ensures the data obtained is of no value.

They cite the example of a user's login and password in which two pieces of unrelated, separate data are of no value. Their model involves splitting the data stored into a Public Data Segment (PDS) and a Sensitive Data Segment (SDS), and SDS data needs to be fragmented still further, until each fragment does not have any value individually. This data is split using the algorithm they describe and explain in such a way that the former ceases to be of any value individually. This model is mainly focused on providing security in avoiding intrusion [38, 40, 41].

In summary, in Table 1 a comparison of the above literature based on the most important parameters as security mechanism and problem tackled is shown.

*3.2. Proposed Security Solution.* The literature review, the comparison, and the analysis help in proposing the theoretical approach to put into practice. The environment is explained in [42] where the proposed approach is applicable in healthcare which is the most important sector of every country around the globe. A set of information obtained from different hospitals and clinics located in the province

Table 1: Comparison of different security mechanisms in the literature.

| Publication | Security mechanism | Problem tackled |
|---|---|---|
| Wang et al. (2009) [38] | CP-ABE scheme | Encryptor leakage (leakage of randomness) |
| Cho et al. (2016) [31] | Double layered architecture | Privacy invasion of personal users in big data |
| Liu et al. (2015) [32] | Authenticator-based data integrity verification techniques | Verification of data integrity |
| Fabiano et al. (2015) [33] | OpenSSL encryption package | Level of security of data |
| Yan et al. (2016) [34] | Proxy-based additive homomorphism | Information security of trusted suppliers |
| Zhou et al. (2015) [35] | Chaos stochastic process and the Line Map principle | Image security |
| Hsu et al. [36] | Variant of the Diffie Hellman algorithm | Secure transfer of data |
| Hingwe and Bhanu (2014) [37] | Data encryption or double encryption for sensitive data | Security on cloud |
| Thilakanathan et al. (2014) [39] | ElGamal algorithm | Security in monitoring patients via remote devices |
| Cheng et al. (2014) [16] | Splitting data in fragments and hash function | Security for a cloud supplier |
| Jing (2014) [18] | AES encryption algorithm and RSA algorithm | Security on the cloud |
| Subashini and Kavitha (2012) [40] | Sensitive Data Segment | Ensuring the data |

of Valladolid (Spain) is proposed theoretically in this model, with information about patients being stored by them on a cloud-based storage server. Moreover, this scheme may be used to scale it to any group of hospitals or clinics in any country. To ensure security of the available systems, such as identification cards or firewalls, it is necessary to increase the security of the information being extracted and stored by these systems, because information security is extremely an important issue.

The possible threats considered are as follows: (a) the internal agent belongs to the health system and that is authorized to access the information but uses it nonethically; (b) second one is the intermediary agent, being identified as a member of the group in possession of the stored information from storage systems; and (c) the external agent is the third kind of threat, which may be anyone other than the authorized user of healthcare system. The proposed improvement focuses on improving the security against these three threats.

The information that requires protection is maintained as the set of data expressed in the form of text or images. The first theoretical proposal involves using the double-layer scheme suggested by Subashini and Kavitha (2012), in which the text data is split in such a manner that it is of no use and is of no value. By doing this we obtain a certain anonymity regarding the data, which is an important factor in the area of health [40]. As an alternative, the scheme by Cho et al. (2016) can be used, which involves splitting the data into sensitive and nonsensitive but for the same purpose, that is, to make the information anonymous. The next step will be to use the proposal made by Jing (2014), which describes the use of double encryption in order to protect data [18]. Now that the data has been split, encryption will help to ensure that intermediary and external agents will not obtain information in the format of flat text. The encryption mechanism is utilized specifically to make unauthorized access of the data impossible [43]. Additionally, the algorithm developed by Zhou et al. (2015) can be used for the medical images, due to the fact that it often tends to be preferable not to split into fragments, as these medical images are deemed to be as valuable as written reports and hence need to be protected. The proposed efficient security mechanism ensures that only authorized persons are able to decrypt the images.

In Figure 2, we visually explain the two alternatives put forward in the first stage when splitting the text-based information generated. Whereas encrypting the text and images is the same in both situations, these two alternatives are split into 3 layers, with layer 1 being the lower one that includes the text and images and in layer 3 the data is encrypted. The first layer simply represents the type of information gathered, and in this case the data is the composition of text and images.

On the left side, the technique by Cho et al. (2016) is utilized that splits the text into sensitive and nonsensitive information that represents personal details and in general labels such as "name," respectively. On the other right side, the technique given by Subashini and Kavitha (2012) is used which fragments the text when it is required and stops until it gives value [40]. Furthermore, the proposed scheme fetches the fragmented text and delivers the actual data to the authorized users and hence ensures the security.

In both cases, we maintain the images without either varying or fragmenting owing to the fact that we have at our disposal the algorithm developed by Cho et al. (2016) in order to ensure their efficient encryption and that no fragment of the image can be obtained without the suitable key [31]. All this information that has already been encrypted will be passed via Internet to the cloud servers.

## 4. Conclusion

This article provides different mechanisms and algorithms used to ensure big data security. Some of these techniques to help preserve information security are data modification techniques, cryptographic methods, protocols for data

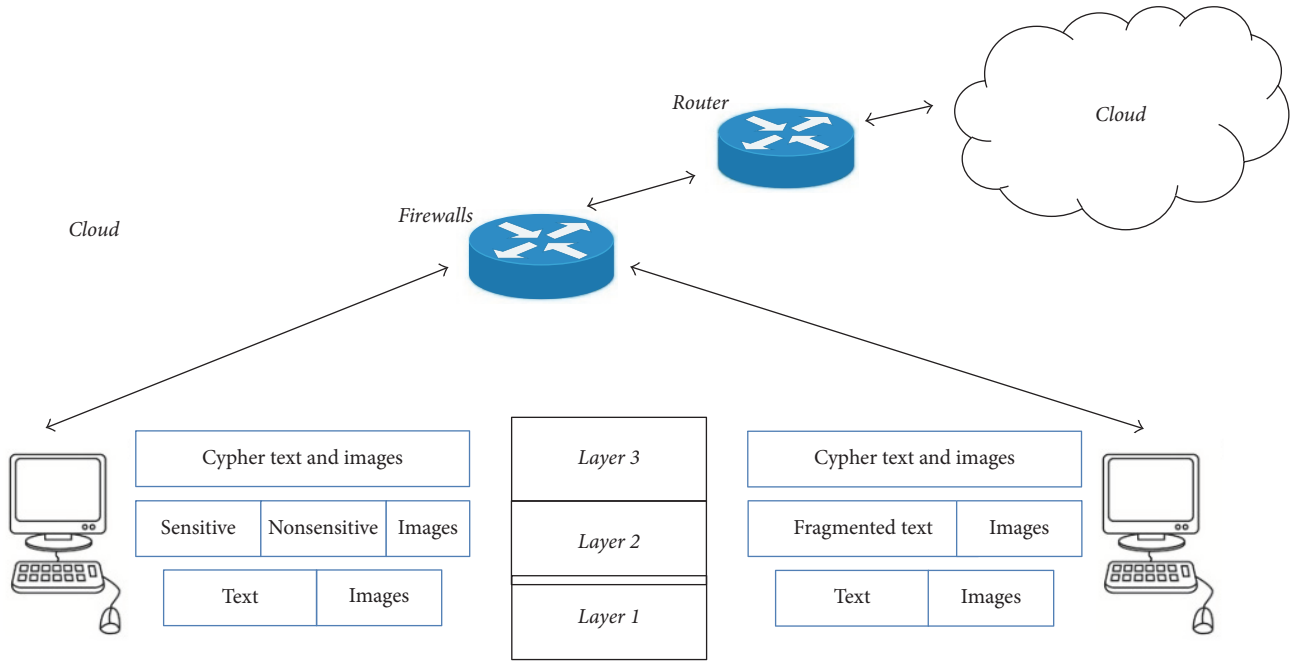


Figure 2: Proposed security scheme.

sharing, and query auditing methods. Although there remains much to do in the field of big data security, research in this area is moving forward, from both a scientific and commercial point of view. Two security alternatives have been proposed theoretically. The new proposed model pretends to give more security on the cloud in hospitals and clinics in Valladolid, Spain.

There is no perfect security system, as the methods currently in use are meant for other applications. Technology has been taking huge steps forward over the years, which may help to create algorithms that cannot currently be used owing to the computational load they require. However, this technology is the same for hackers, meaning that they need increasingly less time to discover the keys. Hence, is security perfect? At present, the only way of remaining beyond the reach of cybercriminals is not to be on the Net, although this of course is not a solution. This is because we are talking about storing data on the cloud, which is something that can be accessed via the Net and whereby disconnecting would mean not gaining access to that data or simply not being able to store it. Should we combine all these mechanisms and security algorithms? This might be one solution; it seem that things depend to quite a large extent on situations in so far as some are health-oriented; others are geared to protecting a database and others to protecting the very keys that encrypt the data being stored. One of these ways is the one we have proposed here which, although far from being perfect, may help to prevent cyber-attacks from the man-in-the-middle.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research has been partially supported by the European Commission and the Ministry of Industry, Energy and Tourism under the project AAL-20125036 named "Wetake-Care: ICT-Based Solution for (Self-) Management of Daily Living," by National Funding from the Fundação para a Ciência e a Tecnologia (FCT) through the UID/EEA/500008/2013 Project, by the Government of the Russian Federation, Grant 074-U01, and by Finep, with resources from Funttel, Grant no. 01.14.0231.00, under the Centro de Referência em Radiocomunicações (CRR) project of the Instituto Nacional de Telecomunicações (Inatel), Brazil.

## References

[1] JM. Martínez Sesmero, ""Big Data"; application and utility for the healthcare system," *Farm Hosp*, vol. 39, no. 2, pp. 69-70, 2015.

[2] D. Shin, T. Sahama, and R. Gajanayake, "Secured e-health data retrieval in DaaS and Big Data," in *Proceedings of the 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services, (Healthcom '13)*, pp. 255–259, IEEE, Lisbon, Portugal, October 2013.

[3] V. A. Chang, "A model to compare cloud and non-cloud storage of Big Data," *Future Generation Computer Systems*, vol. 57, pp. 56–76, 2016.

[4] T. Huang, L. Lan, X. Fang, P. An, J. Min, and F. Wang, "Promises and challenges of big data computing in health sciences," *Big Data Research*, vol. 2, no. 1, pp. 2–11, 2015.

[5] C. L. P. Chen and C. Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: a survey on Big Data," *Information Sciences*, vol. 275, pp. 314–347, 2014.

[6] D. Agrawal, A. El Abbadi, V. Arora et al., "Mind your Ps and Vs: a perspective on the challenges of big data management

and privacy concerns," in *Proceedings of the 2015 International Conference on Big Data and Smart Computing, (BIGCOMP '15)*, pp. 1–6, Republic of Korea, February 2015.

[7] B. Logica and R. Magdalena, "Using big data in the academic environment," *Procedia Economics and Finance*, vol. 33, pp. 277–286, 2015.

[8] A. Gandomi and M. Haider, "Beyond the hype: big data concepts, methods, and analytics," *International Journal of Information Management*, vol. 35, no. 2, pp. 137–144, 2015.

[9] X. Jina, B. Waha, X. Chenga, and Y. Wanga, "Significance and challenges of big data research," *Big Data Research*, vol. 2, pp. 59–64, 2015.

[10] P. Sommer, "DI commentary: big data and privacy," *Digital Investigation*, vol. 15, pp. 101–103, 2015.

[11] Z. Goli-Malekabadi, M. Sargolzaei-Javan, and M. K. Akbari, "An effective model for store and retrieve big health data in cloud computing," *Computer Methods and Programs in Biomedicine*, vol. 132, pp. 75–82, 2016.

[12] MongoDB, https://www.mongodb.com.

[13] Cassandra Apache, "Apache software foundation," http://cassandra.apache.org.

[14] Google BigTable, "Google cloud platform," https://cloud.google.com/bigtable.

[15] W. Tian and Y. Zhao, "Big data technologies and cloud computing," *Optimized Cloud Resource Management and Scheduling Theory and Practice*, pp. 17–49, 2015.

[16] H. Cheng, W. Wang, and C. Rong, "Privacy protection beyond encryption for cloud big data," in *Proceedings of the 2nd International Conference on Information Technology and Electronic Commerce, (ICITEC '14)*, pp. 188–191, IEEE, Dalian, China, December 2014.

[17] F. F. Moghaddam, M. B. Rohani, M. Ahmadi, T. Khodadadi, and K. Madadipouya, "Cloud computing: vision, architecture and characteristics," in *Proceedings of the 6th IEEE Control and System Graduate Research Colloquium, (ICSGRC '15)*, pp. 1–6, IEEE, Shah Alam, Malaysia, August 2015.

[18] P. Jing, "A new model of data protection on cloud storage," *Journal of Networks*, vol. 9, no. 3, pp. 666–671, 2014.

[19] N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "A multi-tenant cloud-based DC nano grid for self-sustained smart buildings in smart cities," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 14–21, 2017.

[20] I. de la Torre-Díez, B. Garcia-Zapirain, M. López-Coronado, and J. J. Rodrigues, "Proposing telecardiology services on cloud for different medical institutions: a model of reference," *Telemedicine and e-Health*, vol. 23, no. 8, pp. 654–661, 2017.

[21] Y. Wen, X. Zhu, J. J. P. C. Rodrigues, and C. W. Chen, "Cloud mobile media: reflections and outlook," *IEEE Transactions on Multimedia*, vol. 16, no. 4, pp. 885–902, 2014.

[22] C.-W. Tsai and J. J. P. C. Rodrigues, "Metaheuristic scheduling for cloud: a survey," *IEEE Systems Journal*, vol. 8, no. 1, pp. 279–291, 2014.

[23] R. Samani, B. Honan, and J. Reavis, "Cloud security alliance research," *CSA Guide to Cloud Computing*, pp. 149–169.

[24] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "A dynamic prime number based efficient security mechanism for big sensing data streams," *Journal of Computer and System Sciences*, vol. 83, no. 1, pp. 22–42, 2017.

[25] M. R. Aswin and M. Kavitha, "Cloud intelligent track - Risk analysis and privacy data management in the cloud computing," in *Proceedings of the International Conference on Recent Trends in Information Technology, (ICRTIT '12)*, pp. 222–227, IEEE, Chennai, India, April 2012.

[26] D. Hodges and S. Creese, "Breaking the arc: risk control for big data," in *Proceedings of the 2013 IEEE International Conference on Big Data, (Big Data '13)*, pp. 613–621, IEEE, Santa Clara, California, USA, October 2013.

[27] IEEE Xplore Digital Library, http://ieeexplore.ieee.org/search/advsearch.jsp.

[28] Scopus, http://www.scopus.com.

[29] Science Direct, http://www.sciencedirect.com.

[30] Web of Science, https://apps.webofknowledge.com/UA_General_Search_input.do?product=UA&search_mode=GeneralSearch&SID=X1MambjOfgrnGY3sm74&pref.

[31] D.-E. Cho, S. J. Kim, and S.-S. Yeo, "Double privacy layer architecture for big data framework," *International Journal of Software Engineering & Applications*, vol. 10, no. 2, pp. 271–278, 2016.

[32] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: a big picture," *Future Generation Computer Systems*, vol. 49, pp. 58–67, 2015.

[33] E. Fabiano, M. Seo, X. Wu, and C. C. Douglas, "OpenDBDDAS toolkit: secure mapreduce and hadoop-like systems," *Procedia Computer Science*, vol. 51, pp. 1675–1684, 2015.

[34] Z. Yan, W. Ding, V. Niemi, and A. V. Vasilakos, "Two schemes of privacy-preserving trust evaluation," *Future Generation Computer Systems*, vol. 62, pp. 175–189, 2016.

[35] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[36] C. Hsu, B. Zeng, and M. Zhang, "A novel group key transfer for big data security," *Applied Mathematics and Computation*, vol. 249, pp. 436–443, 2014.

[37] K. K. Hingwe and S. M. S. Bhanu, "Sensitive data protection of DBaaS using OPE and FPE," in *Proceedings of the 4th International Conference on Emerging Applications of Information Technology, (EAIT '14)*, pp. 320–327, Kolkata, India, December 2014.

[38] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *Proceedings of the 17th International Workshop on Quality of Service (IWQoS '09)*, pp. 1–9, IEEE, Charleston, SC, USA, July 2009.

[39] D. Thilakanathan, Y. Zhao, S. Chen, S. Nepal, R. A. Calvo, and A. Pardo, "Protecting and Analysing Health Care Data on Cloud," in *Proceedings of the 2nd International Conference on Advanced Cloud and Big Data, (CBD '14)*, pp. 143–149, IEEE, Huangshan, China, November 2014.

[40] S. Subashini and V. Kavitha, "A metadata based storage model for securing data in cloud environment," *American Journal of Applied Sciences*, vol. 9, no. 9, pp. 1407–1414, 2012.

[41] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[42] I. De La Torre-Díez, M. Lopez-Coronado, B. Garcia-Zapirain Soto, and A. Mendez-Zorrilla, "Secure cloud-based solutions for different eHealth services in spanish rural health centers," *Journal of Medical Internet Research*, vol. 17, no. 7, article no. e157, 2015.

[43] Z. Wang, C. Cao, N. Yang, and V. Chang, "ABE with improved auxiliary input for big data security," *Journal of Computer and System Sciences*, vol. 89, pp. 41–50, 2017.