A Survey of Big Data Security Solutions in Healthcare

Musfira Siddique[1], Muhammad Ayzed Mirza[1], Mudassar Ahmad[1(✉)], Junaid Chaudhry[2], and Rafiqul Islam[3]

[1] Department of Computer Science, National Textile University, Faisalabad, Pakistan
musfirasiddique@ymail.com, ayzed@ntu.edu.pk, mudassar.utm@gmail.com
[2] Cyber Security Faculty, Cyber Intelligence and Security Department College of Security and Intelligence, Embry-Riddle Aeronautical University Prescott, Prescott, AZ, USA
chaudhrj@erau.edu
[3] School of Computing and Mathematics, Charles Sturt University, Bathurst, NSW 2795, Australia
mislam@csu.edu.au

Abstract. Today data is a strategic asset and organizational goal is to maximize the value of their information. The concept of big data is now treated from different points of view covering its implications in many fields remarkably including Healthcare. Healthcare data is progressively being digitized and the Healthcare era is expansively using new machineries. Thus the medical data is increasing day by day has reached a momentous size all over the world. Although this data is being addressed as the basic to offer treasured insights and sinking cost, the security and privacy issues are so irresistible that medical industry is not capable to take full benefit of it. Privacy of Healthcare is a significant feature overseen by medical acts thus, the data must be secured from dwindling into the wrong hands or from being hacked. Due to the growing threats of loss and outflows from personal data and augmented acceptance of cloud technologies it is important to secure current Healthcare big data domain. This paper aims to present the state-of-the-art security and privacy issues in big data as pragmatic to Healthcare industry and discuss some available data privacy, data security, users' access control mechanisms and approaches.

Keywords: Big data · Cloud · Healthcare · Security · Analytics

1 Introduction

Big data is data sets that are so voluminous and complex that cannot be analyzed with traditional computing techniques. Big data philosophy encompasses unstructured, semi-structured and structured data, however the core concentration is on unstructured data [1]. Data that is unstructured or time sensitive or simply very large cannot be handled by relational database engines. Quite

R. Beyah et al. (Eds.): SecureComm 2018, LNICST 255, pp. 391–406, 2018.
https://doi.org/10.1007/978-3-030-01704-0_21

simply, big data reflects the changing world we live in. The more the variations are taken and documented as data as the more things alternate. Take Facebook as an example, Facebook handles almost 40 billion photos from its user base it also handles audio and video data, per second. There are many Twitter tweets handled per second and also YouTube data is generating enormously. Other examples are Cloud and web data, social media data, time and location data, scientific instruments and sensors data. Data has grown speedily, as of 2012, every day 2.5 exabytes (2.5×1018) of data are generated. By 2025, International Data Corporation (IDC) predicts there will be 163 zettabytes of data. Big data is often characterized by its three V's. The extreme volume of data, the wide variety of data types and the velocity at which the data must be processed [2]. And some even extend this to five Vs and currently its extended to ten Vs shown in Fig. 1 and defined as follows [3–8]:

1.1 V's of Big Data

- ***Volume:*** Volume is the amount of data. While volume specifies more data, the data is generated from web, sensors, social media etc. It refers to the amount of data generated after every second and classify as records, tables and files.
- ***Velocity:*** Velocity is the fast rate at which data is received and possibly proceeded. It is the in and out flow of data, the data upload and download time and data at motion. It includes Batch velocity, near time data, Real time Data and Social media data.
- ***Variety:*** Variety is the many forms of data. Like Structured, Unstructured, semi-structured and multi-structure data types. Data such as text, audio, and video need supplementary processing to both originate denotation and the subsidiary metadata.
- ***Variability:*** In bigdata's context, variability refers to different things. One is inconsistencies/outliers in data. It is also variable due to multitude dimensions of variables resulting from various data sources and dissimilar data types. It also refers to variable frequency of bigdata to be loaded into database.
- ***Veracity:*** Veracity refers to the confidence to trust in data. This one is the unfortunate part of bigdata. As most of the other characteristics are in increasing trend but it drops. It refers more to the provenance or reliability of the data source, its context, and how meaningful it is to the analysis based on it. It helps us to determine the risk associated with the analysis or decision made based on a particular dataset.
- ***Validity:*** Much like veracity, validity refers to how correct and valid/accurate data is to be used for the task. Scientist's approximately 60% of time is consumed to refine the data for what they conduct analysis. The analytical advantage from bigdata is only as good as its primary data. There is a need to have a good data governance practices to ensure consistent data class and metadata.
- ***Vulnerability:*** Everybody is cautious regarding data security. Bigdata has also got new security concerns. If bigdata is breached it would be a colossal

data breach. E.g. AshleyMedison hack in 2015 and in May 2016, 167 million LinkedIn profiles and 360 million user passwords of MySpace hack had been reported in the past. So it is a question mark against bigdata vulnerability.

- ***Volatility:*** Data volatility belongs to the data life, how old data should have to be kept before it is considered as irrelevant. Or can say the data-age when data is not useful. Due to huge amount of data in bigdata data volatility is considered as an important and considerable point. Otherwise organizations don't bother to keep data for the life time archives and in live databases without hindering the performance. Rules for data availability, need and clear relationship of data with business process are to be defined for rapid and cost-effective retrieval of information. Bigdata magnifies the complexity the storage cost and retrieval process that's why data volatility is needed.
- ***Visualization:*** It includes the data visualization tools and techniques. Developing a meaningful visualization from the huge multitude variables and their complex relationships of big data. It's not an easy task to visualize that huge and complex data. The traditional ways of graphing and plotting are not sufficient, so different ways of representing data is needed. It may include data clustering, tree maps, sunbursts, parallel coordinates, circular network diagrams, or cone trees.
- ***Value:*** The most important of all is value, is the data into money it denotes the scientific value attributed to this data.

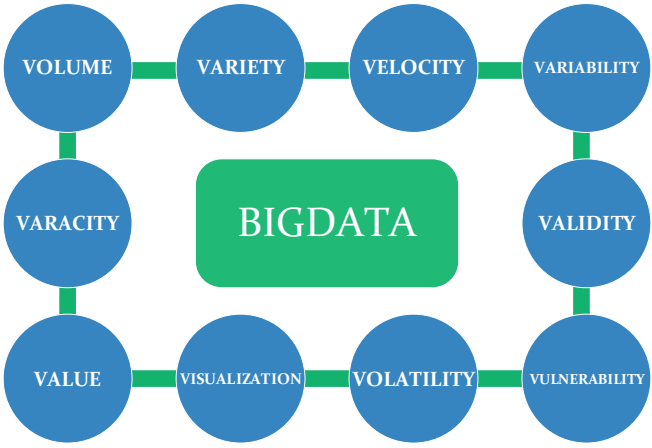

Fig. 1. Vs of big data

The importance of big data doesn't revolve around how much data you have, however what you do with it. You can take data from any source and it to find answers that enable cost reductions, time reductions, new product development and optimized offerings, and smart decision making. Data in its raw form has no

value. Data needs to be processed in order to be of valuable. Processing information like this illustrates why big data has become so important. Unstructured data needs enormous storage and processing, the Internet is increasing the raw data day by day that needs to be processed [9].

There are many major issues related to big data. Big data analysis is one of them, which is the process to uncover hidden patterns and unknown correlations for actual decision making and better strategic moves. Others are big data Security issues, big data management, Data Visualization, Data integration, Transition of big data to the cloud, new ways and technologies to protect big data, Mining Big data, Processing issues, Gaining maximum value from big data and predictive analytics. Some hot topics related to big data are Real time big data analytics, IOT and Big data, big data security, big data in health care and many more [10,11].

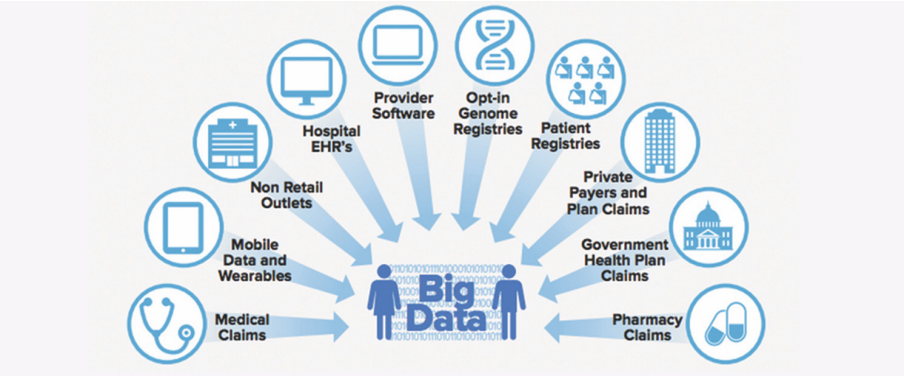

Fig. 2. Big data in Healthcare [12]

1.2 Healthcare Big Data

Generally the Healthcare data includes the patient data and elementary information, clinical data and doctors' data. However now a days the Healthcare era is expansively using new machineries such as apprehending devices, sensors, electronic health records and mobile computing etc. Thus the medical data is increasing day by day the volume of Healthcare data is rapidly increasing. Healthcare data is generating from internal and external sources like biometric data, genetics, blood pressure, electronic medical records, remote sensors data and social media data. All the electronic Healthcare data, patient medical records, surgeries results, medical images data, sensors data and all other medical related data is added into Healthcare database and increasing its size to a great extent [13]. This Healthcare data requires better real time analysis for meaningful information.

Big data analytics has many benefits in Healthcare as it embeds better decision making and reduce cost, it gives benefits to doctors and Healthcare providers, perceiving dispersal diseases earlier, fraud detection, and evidence based medicine and many more. Figure 2 reflects the bigdata involvement in healtcare system [12].

Healthcare data includes many challenges like Comfort of understanding unstructured data and its use, mining hypothetically valuable information from data in order to minimize faults, scalability, Reduction of cost in scrutinising genomics data and mixing this type of data with other information is of great importance, by using many sensors recording patients' interactive data is of great complexity. Above all the vital challenge in perspective of Healthcare domain is the Security issue in Healthcare systems.

Security of the Healthcare Information System is the key concern from the day one. Individual's information must be protected from loss and from hackers attack by using different physical security mechanism and techniques like encryption, authentication, cryptographic algorithms etc. The main root of the security issue is the use of Cloud in Healthcare systems as all the data storage is on cloud and it provides different storage and processing facilities. Hence we should tackle the security problem of Healthcare systems.

2 State-of-the-Art

Nowadays the backbone to the current storage devices is big data and Cloud Computing. As E-Health has grown rapidly and its databases contains voluminous data. The security and privacy preservation is the key concern in this respect. Cloud computing security is very important. The quality of Healthcare should be increased by its security. They proposed a secure e-health framework using hadoop Map reduce data that provides security for Healthcare. Proposed a new framework, Multi Authority Attribute based Encryption (MA-ABE) for securely transferred the PHI to health services after security checks. The encryption technique, Cipher Policy Attribute Based (CP-ABE) was used in it. The research concentrations are with safeguarding health care from outbreaks by illegal users and also detects the intimidations in health care. Accuracy, efficiency and consistency are the performance parameters in the proposed solution. To store the patient medical information securely any organization can use this application as it used the best encryption technique. Also the efficiency of this system is saleable as compared to existing system [14].

The modern Health Information Technology (HIT) electronically preserve and transfer data globally in seconds and offers quality of service to Healthcare. Thus by given the Electronic Medical Records (EMR) to every service provider the main problem with the modern EMRs is that they are potentially centralized. Patients' health information reclamation is a challenge. The aptitude to generally access all patient Healthcare information in an appropriate fashion is of highest importance. Health information must be available and obtain- able to

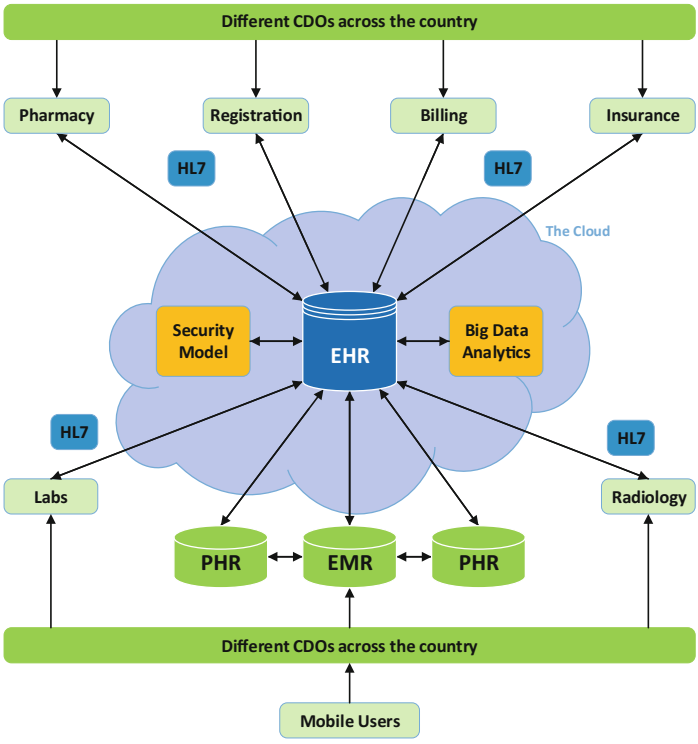

Fig. 3. A framework for secure Healthcare system [15]

everyone tangled in the system. Thus, in order to deliver high-quality Healthcare to the patients they serve a high level of data integration, and sharing among different Healthcare specialists and organizations is essential. Among different Healthcare providers, practitioners and patients the proposed framework offers high level of integration, availability and sharing of data between them. The detailed framework is shown in Fig. 3. Mobile Cloud permits rapid Internet access and endowment of EHRs from everyplace and at any time by altered platforms. The proposed framework employs big data analytics to find useful insights that help specialists proceeds acute decisions in the right time. It applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical information [15].

Gunamalai et al. proposed a method of security and privacy of Personal Medical Records and Digital Imaging and Communication in Medicine (DICOM) images in the Cloud environment. DICOM discourses dissemination and inspecting medical images and also is a typical rule for medical imaging. The penalty area is to enable numerous medical centers to admittance individuals' data for treatment in a protected method. The structure untraceably implants remote patient data like name and exclusive ID in the medical images. Access Governor

is done via two-way authentication. In Two way authentication firstly the user log on by entering correct id and password and secondly the user has to enter the key sent to him after login on his mobile with in a given time period. Thus in this way the user will be verified and get access to cloud data storage. By using Column based encryption Healthcare centres can encrypt their PMR and images to allow granule access. By using column based encryption the user who know the encrypted password can access the specific columns' data. Column Based Encryption (CBE) permits discerning division of data amongst medical centers [16].

Security of patient data is vital in cloud based big data cooperative structure where they offer a platform for sharing and exchanging information exist in different clouds for numerous errands. There is a proposed scheme which is a two phase security protocol that uses pairing based cryptography. Secret data is shared by computing a secret session key which is dynamically generated for every new data-exchange session by computing a pairing in elliptic curve. Hence each new session is no dependent on the previous one. It also gives security against man-in-the-middle attack. Response time, memory and availability are the performance parameters in the proposed solution [17].

Medical content security need is increasing by the extended use of Healthcare management systems. The authors proposed an authentication based access control mechanism for medical content DICOM. The confidentiality of the DICOM in public cloud is ensured by the Access control mechanism. It also provides the integrity of the user detail in Healthcare system [18].

As the EMR of patient need to be accessed by the Healthcare experts. For the ease of access the EMRs need to be stored at Healthcare cloud in big data storages. However the key concern with the Healthcare cloud is its security as the patients sensitive information needs to be secure because data stealing outbreaks are well-thought-out to be one of the vital security breaks Clouds Healthcare data. By using a decoy technique with fog computing facility they present a methodology to prevent patient MBD in Healthcare cloud. Decoy files retrieved at the start thus, as to make system secure by hiding the original file. It uses a double security technique by the encryption of genuine file to prevent system from attackers. Key generation time, accuracy and availability are the performance parameters in the proposed solution. As a result, the proposed methodology guarantees that the MBD of users are 100% protected and reduces the process [19].

Big data contains voluminous amount of data which is growing rapidly day by day. However the booming of big data also hinges on fully accepting and handling newly rising safety and confidentiality trials. The security and privacy preservation of big data is the key concern. New extracted information will be unpersuasive if data is not reliable, while if confidentiality is not well addressed, people may be disinclined to share their data. This have introduced an efficient and privacy-preserving cosine similarity computing protocol in response to the efficiency and privacy requirements of data mining in the big data era. Although have analyzed the privacy and efficiency challenges in general big data analytics

to shed light on the privacy research in big data, significant research efforts should be further put into addressing unique privacy issues in some specific big data analytics. Encrypt/decrypt time, speed and de-identification are the performance parameters in the proposed solution [20,21].

The modern Health Information Technology (HIT) electronically preserve and transfer data globally in seconds and offers quality of service to Healthcare. Thus by given the EMR to every service provider the main problem with the modern EMRs is that they are potentially centralized. Patients' health information reclamation is a challenge. The aptitude to generally access all patient Healthcare information in an appropriate fashion is of highest importance. The first contribution of this research is the provision of an overall picture on big data and Healthcare data for non-expert readers. The other one is the adoption of a holistic view to build an organized Healthcare model for protecting patient data. The model provides high-level integration and sharing of EHRs. The suggested framework as shown in Fig. 4 applies a set of security constraints and access control that guarantee integrity, confidentiality and privacy for medical data [22].

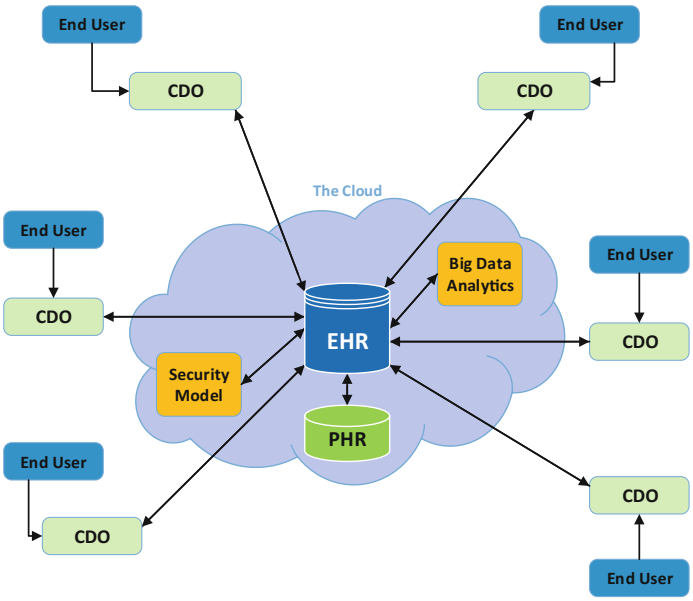

Fig. 4. A framework for distributed Health system [22]

Security is a key concern in Remote Patient Monitoring framework as there is a little evidence on this problem's solution. The authors proposed a new security framework for Patient Remote Monitoring devices which is a wide-ranging model. They projected NFC technology to tackle the problem of multi user device patient identification. Firstly a patient identifies using NFC no and take their

Table 1. Comparison of different security mechanism

Sr. No	Author	Problem tackled	Security mechanism	Performance parameters
1	B. Prasanna et al.	Big data and Cloud security	CP-ABE scheme	Response time, accuracy
2	Ahmed E. Youssef	Mobile cloud security,	AES and RC4 encryption	Key generation time, response time, encrypt/decrypt time
3	Gunamalai et al.	Information security	Two way authentication and CBE	Tate pairing time, memory
4	Mehedi et al.	Big data and Cloud	Pairing based cryptography	Confidentiality, integrity
5	Subhasri et al.	Security	Authentication based access control mechanism	Response time, memory requirement, accuracy
6	Hadeal Abdul aziz et al.	Big data security in	Fog computing with pairing based cryptography	Key generation time, integrity, speed
7	Sathya et al.	Collaborative environment	Triple DES	Integrity, confidentiality, availability
8	Bikash Kanti Sarkar	DICOM content	AES and RC4 encryption	Authentication, availability
9	Brian Ondiege et al.	Security in cloud	NFC for identification	Authentication, availability
10	Chao YANG et al.	Big data and Cloud	triple encryption method	Encrypt/decrypt time, memory
11	Rui Zhang, Ling Liu	Big data Cloud security	Attribute-based Composite, encryption	Response time, memory requirement, accuracy
12	Ali Gholami and Erwin Laure	Cloud security	NFC for identification, DES etc	Integrity, confidentiality, availability
13	B. Vinoth Kumar et al.	Patient monitoring security (IOT and Cloud)	AES and DES encryption	Key generation time, memory used, availability
14	Weiwei LIN et al.	Data security WBANs	Multi biometric based key generation scheme	Confidentiality, integrity
15	Farrukh Aslam Khan et al.	Remote patient monitoring security	NFC for identification	Integrity, confidentiality, availability

B.P reading. Then system checks if that patient exists and able to send its reading, thus it will continue its procedure. The also enable capability system which allows only registered devices to send their readings via secure communication protocol. They uses the performance parameters like accuracy, availability and memory used [23].

As Healthcare data is increasing rapidly and it need better storage, for this purpose cloud is used. However the security of the data in cloud is a threat. To address this problem the authors proposed a Novel Triple Encryption method. In the triple encryption scheme, HDFS files are encrypted by using the hybrid encryption based on DES and RSA, and the user's RSA private key is encrypted using IDEA. The triple encryption scheme is implemented and integrated in Hadoop-based cloud data storage. Encrypt/decrypt time, memory and availability are the performance parameters in the proposed solution. Results of experiment show that the triple encryption scheme is feasible, it meets the reading and writing characteristics of HDFS and can enhance the confidentiality of default HDFS [24]. Table 1 shows a summarized comparison of different security algorithms proposed by different researchers.

3 Big Data Security Solutions in Healthcare

The main security models discussed in this paper are related to big data Healthcare and cloud, big data and IOT in Healthcare and securing patient data in cloud and big data architectures.

3.1 Cloud and Big Data in Healthcare

Cloud computing is a shared pool of configurable computing resources. Now a days for handling of Healthcare data and Healthcare information classifications cloud computing in comprehensively used [13]. As Healthcare organizations has been moved to electronic platform today from where it gathers amply of data. The significant amount of data need to be stored and processed. Cloud computing is best suited for Healthcare domain. It provides many benefits as it makes data sharing easy and more handy for the user, it provides cost reduction operations. However with the electronic medical records there is a chance of data loss and other information loss. Cloud computing sideways with Big Data tools has Initiate use in Curative Imaging, clinic organization and Healthcare Information Systems, public health and individual's self-service applications. With the rising use of cloud computing tools in Healthcare it is authoritative that, security of Healthcare data in the cloud is a key concern that needs to be well-kept-up sideways with secure the cloud computing.

Fog Computing Facility with Pairing-Based Cryptography
Fog computing, is an evolving model that offers storing, dispensation, and communication amenities nearer to the end user. Providing data and tapping them on the upper hand of a network to be closer to the user are well-thought-out amongst the main tasks of fog computing. The proposed method as shown in Fig. 5 provide the user's multimedia data security by using fog computing. A well-organized tri-party genuine key covenant protocol has been proposed based on paring cryptography among the user, the DPG, and the OPG. This is an illusion technique as it provides the attacker a decoy gallery rather than the original one. As shown in figure when the user log on whether it is an attacker

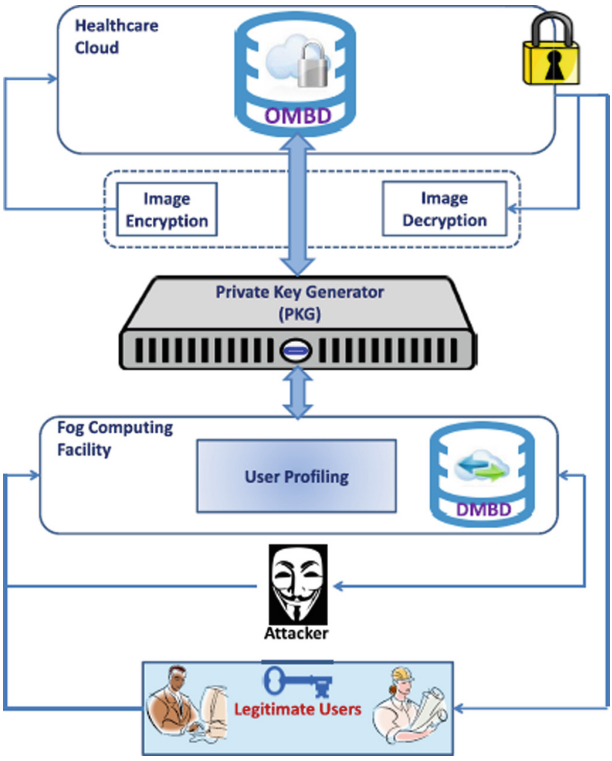

Fig. 5. Proposed security framework using fog computing facility [19]

or legitimate user it will be shown the DMBD which is a decoy gallery. Then the second step will be the verification of the legitimate user as he knows that DMBD is fake thus, he will access original OMBD by verifying himself. Thus in this way the original MBD will remain safe from hackers. The algorithms used are DMBD algorithm, Key exchange algorithm, user profiling algorithm and photo encryption and decryption algorithm [19].

Two Way Authentication and Column Based Encryption

Authentication is a process of identifying the user who has stances the rights to access and modify data on cloud. In Two way authentication firstly the user log on by entering correct id and password and secondly the user has to enter the key sent to him after login on his mobile with in a given time period. Thus in this way the user will be verified and get access to cloud data storage. By using Column based encryption Healthcare centers can encrypt their PMR and images to allow granule access. By using column based encryption the user who know the encrypted password can access the specific columns' data. Hence it allows many Healthcare centers to access patients' data for treatment in a secure way. Figure 6 shows a scenario in which multiple centers can access multiple columns by using the secret key [16].

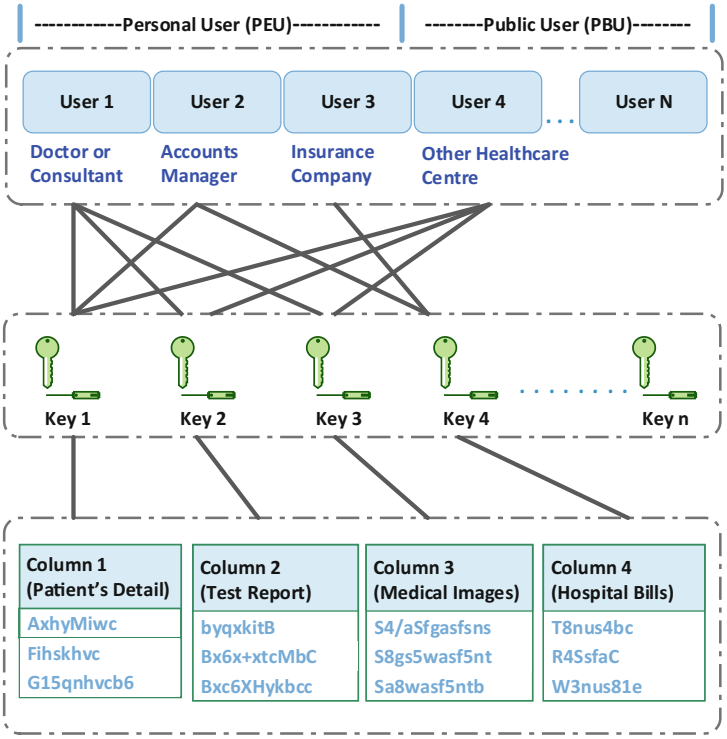

Fig. 6. Proposed security framework using column based encryption [16]

3.2 IOT and Big Data in Healthcare

To monitor the medical disorder of patient Wireless Body Area Networks or WBANs are used by using miniature sensor bulges entrenched to the human body. Wireless Sensor Network (WSN) is developed by these sensor bulges. From the human body the biological information is sent to a regulator device either devoted to the human body or in the 90 locality wirelessly. Then for more analysis the gathered data is sent to isolated servers or cloud of a hospital/Healthcare center. WBANs can be used for blood flow, ECG, pulse rate, blood pressure, body temperature etc. It is vigorous to guarantee precision and veracity of such Healthcare data [29–31]. Hereafter security and privacy of WBANs must be safeguarded. Security must be preserved for WBANs in the attached sensors to the body, isolated servers where WBAN data is pushed, communication medium.

Multi Biometric Based Key Generation Process for Securing WBANs In patient monitoring the patients' data is gathered though the sensors attached to the patients' body and sent to the remote servers for further actions. Multi biometric scheme is used for securely generate the key. It is useful for secure inter sensor communication. Features are selected from ECG and EEG values and quantized hence divide in blocks and exchanged by applying key hashing. At

the receiving end the key generation algorithm is applied for extraction of information and then both the sensor nodes use this key for secure communication [23]. The flow of security framework is shown in Fig. 7. In patient monitoring the patients' data is gathered though the sensors attached to the patients' body and sent to the remote servers for further actions. Multi biometric scheme is used for securely generate the key. It is useful for secure inter sensor communication. Features are selected from ECG and EEG values and quantized hence divide in blocks and exchanged by applying key hashing. At the receiving end the key generation algorithm is applied for extraction of information and then both the sensor nodes use this key for secure communication. Then for more analysis the gathered data is sent to isolated servers or cloud of a hospital/Healthcare center. WBANs can be used for blood flow, ECG, pulse rate, blood pressure, body temperature etc. It is vigorous to guarantee precision and veracity of such Healthcare data. Hereafter security and privacy of WBANs must be safeguarded. Security must be preserved for WBANs in the attached sensors to the body, isolated servers where WBAN data medium.

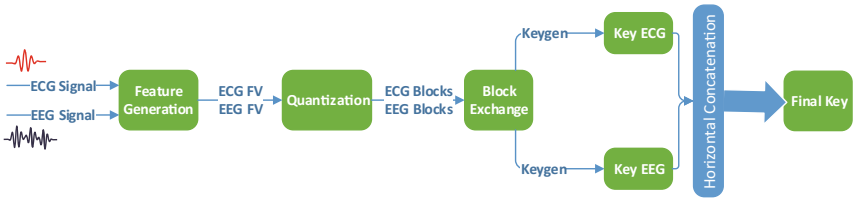

Fig. 7. Proposed security framework using multi biometric based key generation [23]

4 Discussion

In this paper, i have examined the security and privacy challenges in big data, by deliberating some existing mechanisms and techniques for achieving security and privacy in which Healthcare administrations are likely to be highly beneficial. The security challenges mainly include the security of patient data on cloud, the secure sharing of data in cloud collaborative environments, protect the patient medical records, sensors data security in remote patient monitoring systems, and information security. Many techniques were used to tackle these challenges like triple encryption, pairing based cryptography, CP-ABS mechanism, fog computing, two way authentication and Column based encryption and authentication based access control mechanism. From all of these Fog computing Technique with Pairing based Cryptography, two way authentication and CBE have shown better results. Future work may include to take one of these mechanism and apply it on some dataset to improve the security on cloud.

5 Conclusion

While Big Data technologies are improving day by day this also means that the volume of data along with the rate at which data is flowing into enterprises today is increasing. Healthcare data is progressively being digitized now a days the Healthcare era is expansively using new machineries such as apprehending devices, sensors, electronic health records and mobile computing etc. Thus the medical data is increasing day by day has reached a momentous size all over the world. Although this data is being addressed as the basic to offer treasured insights and sinking cost, the security and privacy issues are so irresistible that Medical industry is not capable to take full benefit of it. Privacy of Healthcare is a significant feature overseen by Medical Acts thus, the data must be secured from dwindling into the wrong hands or from being hacked. Due to the growing threats of loss and outflows from personal data and augmented acceptance of cloud technologies it is important to secure current Healthcare big data domain. This paper aims to present the state of- the-art security and privacy issues in big data as pragmatic to Healthcare industry and discuss some available data privacy, data security, users' access control mechanisms and approaches.

References

1. Martınez Sesmero, J.M.: Big data application and utility for the healthcare system. FarmHosp **39**(2), 69–70 (2015)
2. Shin, D., Sahama, T., Gajanayake, R.: 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 2013), pp. 255–259. IEEE, Lisbon, Portugal, October 2013
3. Chang, V.A.: Amodel to compare cloud and non-cloud storage of big data. Future Gener. Comput. Syst. **57**, 56–76 (2016)
4. Huang, T., Lan, L., Fang, X., An, P., Min, J., Wang, F.: Promises and challenges of big data computing in health sciences. Big Data Res. **2**(1), 2–11 (2015)
5. Firican, G.:The 10 Vs of Big Data, TDWI, 8 February 2017. https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx. Accessed 23 Apr 2018
6. Chen, C.L.P., Zhang, C.Y.: Data-intensive applications, challenges, techniques and technologies: a survey on big data. Inf. Sci. **275**, 314–347 (2014)
7. Logica, B., Magdalena, R.: Using big data in the academic environment. Procedia Econ. Financ. **33**, 277–286 (2015)
8. Agrawal, D., El Abbadi, A., Arora, V.,et al.: Mind your Ps and Vs: a perspective on the challenges of big data management 6 wireless communications and mobile computing and privacy concerns. In: Proceedings of the 2015 International Conference on Big Data and Smart Computing, (BIGCOMP 2015), pp. 1–6, Republic of Korea, February 2015
9. Sabar, N.R., Abawajy, J., Yearwood, J.: Heterogeneous cooperative co-evolution memetic differential evolution algorithm for big data optimization problems. IEEE Trans. Evol. Comput. **21**(2), 315–327
10. Jina, X., Waha, B., Chenga, X., Wanga, Y.: Significance and challenges of big data research. Big Data Res. **2**, 59–64 (2015)

11. Mirza, M.A., Habib, M.A.: Optimized energy ingestion in IoT enabled sensor nodes: a survey. J. Softw. Eng. Intell. Syst. **2**(3), 3 (2017). E-ISSN: 2518–8739
12. Big data in HealthCare. https://www.google.com/imgres?imgurl=http
13. Widmer, A., Schaer, R., Markonis, D., Müller, H.: Gesture interaction for content-based medical image retrieval. In: Proceedings of the 4th ACM International Conference on Multimedia Retrieval, pp. 503–506. ACM, New York (2014)
14. Jina, X., Waha, B., Chenga, X., Wanga, Y.: E-health for security and privacy in health caresystem using hadoop map reduce. Big Data Res. **2**, 59–64 (2015)
15. Youssef, A.E.: A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. Int. J. Ambient Syst. Appl. (IJASA) **2**(2) (2014)
16. Gunamalai, C., Sivasubramanian, S.: Novel method of security and privacy for personal medical record and DICOM images in cloud computing. ARPN J. Eng. Appl. Sci. **2**, 59–64 (2015)
17. Masud, M., Hossain, M.S.: Secure data-exchange protocol in a cloud-based collaborative health care environment. Big Data Res. **2**, 59–64 (2017)
18. Subhasri, P., Padmapriya, A.: Authentication based access control mechanism for ensuring privacy of DICOM contents in public cloud. Aust. J. Basic Appl. Sci. **11**(10), 128–136 (2017)
19. Al Hamid, H.A., Mizanur, Sk. Md.: A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access **2**, 59-64 (2016)
20. Sathya, S., Sethukarasi, T.: Efficient privacy preservation technique for healthcare records using big data. In: International Conference On Information Communication And Embedded System (ICICES 2016) (2016)
21. Victor, N., Lopez, D., Abawajy, J.H.: Privacy models for big data: a survey. Int. J. Big Data Intell. **3**(1), 61–75
22. Sarkar, B.K.: Big data for secure healthcare system: a conceptual design. Big Data Croos Mark **2**, 59–64 (2017)
23. Ondiege, B., Clarke, M., Mapp, G.: Exploring a new security framework for remote patient monitoring devices. Big Data Res. **2**, 59–64 (2017)
24. Yang, C., Lin, W., Liu, M.: A novel triple encryption scheme for hadoop-based cloud data security. In: 2014 Fourth International Conference on Emerging Intelligent Data and Web Technologies (2014)
25. Zhang, R., Liu, L.: Security models and requirements for healthcare application clouds. In: 2017 Fourth International Conference on Emerging Intelligent Data and Web Technologies (2017)
26. Gholami, A., Laure, E.: Security and privacy of sensitive data in cloud computing: a survey of recent developments, vol. 2. Springer (2016)
27. Vinoth Kumar, B., Ramaswami, M., Swathika, P.: Data security on patient monitoring for future healthcare application. Int. J. Comput. Appl. **163**(6), 0975–8887 (2017)
28. Khan, F.A., Alia, A., et al.: A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. In: The 2nd International Workshop on Communications and Sensor Networks (ComSense-2014) (2014)
29. Chaudhry, J.A., Tariq, U., Amin, M.A., Rittenhouse, R.G.: Sinkhole vulnerabilities in wireless sensor networks. Int. J. Secur. Appl. **8**(1), 401–410 (2014)
30. Rittenhouse, R.G., Chaudry, J.A., Lee, M.: Security in graphical authentication. Int. J. Secur. Appl. **7**(3), 347–356 (2013)

31. Jabbar, S., Ahmad, M., Malik, K.R., Khalid, S., Chaudhry, J., Aldabbas, O.: Designing an energy-aware mechanism for lifetime improvement of wireless sensor networks: a comprehensive study. Mobile Netw. Appl. **23**, 1–14 (2018)
32. Malik, K.R., Farhan, M., Habib, M.A., Khalid, S., Ahmad, M., Ghafir, I.: Remote access capability embedded in linked data using bi-directional transformation: issues and simulation. Sustain. Cities Soc. **38**, 662–674 (2018)