ISSN No: - 2456 – 2165

Big Data Security in Healthcare

Jasti Satyakrishna
M.Tech (CS&E)
Amity University Uttar Pradesh

Raj Kumar Sagar
A.P.Grade-1
Amity University Uttar Pradesh

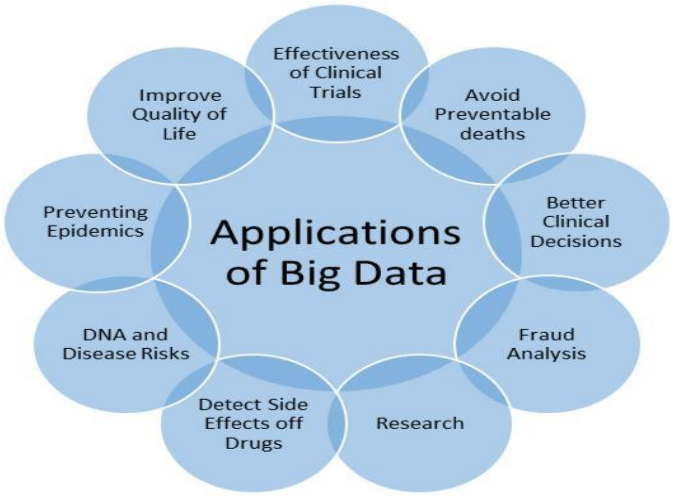
Abstract- Medicinal services information is progressively being digitized today and the information gathered today rolling in from all present day gadgets, has achieved a noteworthy volume everywhere throughout the world. In the US, UK and other European nations, medicinal services information needs to be secured and Patient Health Records (PHR) should be ensured with the goal that re-recognizable proof of patients is impossible from fundamental data. Protection of human services is an essential viewpoint administered by Healthcare Acts (e.g. HIPAA) and henceforth the information should be secured from falling into the wrong hands or from being ruptured by malevolent insiders. It is critical to secure existing medicinal services enormous information conditions due to expanding dangers of breaks and holes from private information also, expanded appropriation of cloud advancements. In this paper the current human services security situation in enormous information conditions has been compressed alongside challenges confronted and security issues that need consideration. Some current methodologies have been portrayed to show present and standard headings to comprehending the issues. Since medicinal services administration in the US has a solid concentrate on security and protection rather than different nations on this day, the paper concentrates on Acts and security hones in the US setting.

Keywords- Health Care, Big Data, Big Data Security, Big Data Privacy.

I. HEALTHCARE AND BIG DATA

With the expanding utilization of innovation and accumulation of social insurance related information by therapeutic suppliers, the volume of information accessible is expanding each day. This information can be profitably utilized for research and examination. These gigantic datasets can be utilized to produce centered information and experiences utilizing prescient examination and BI empowering educated choices in the realm of medicinal services and henceforth conceivably spare patients' lives, make medications financially savvy and make strides operational proficiency.

Utilizations of Big Data in Healthcare include: Counteracting Epidemics – Big Data was utilized as a part of keeping the spread of Ebola infection in Africa by spotting populace developments and giving bits of knowledge to the best territories for setting up treatment focuses and acquire development limitations. Enhance Quality of Life – Smartphone's, applications and wellbeing devices today can gather wellbeing information and give us bits of knowledge for enhancing the personal satisfaction and take essential restorative activity when required. This is finished by transferring the gathered information and incorporating it with existing datasets. This has the possibility to spot issues before they happen and give recommendations for a solid life. Enhance adequacy of Clinical Trials – Huge measures of information on potential contender for clinical trials can be investigated to recognize the best subjects for clinical trials. Stay away from Preventable Deaths – Constant observing of therapeutic conditions can give alarms to make preventive move. Medicinal information can be contrasted with existing informational indexes with come to bits of knowledge on whether there is a hazard. Distinguishing Side Effects of Drugs – Patient information and their restorative conditions over some undefined time frame can prompt bits of knowledge on regardless of whether there are discernible symptoms to a medication. Recognizing Disease Risks from the DNA – Family history on sicknesses and therapeutic conditions can be profiled and DNA examination can give bits of knowledge on restorative conditions a patient is liable to experience.



ISSN No: - 2456 – 2165

Furnish Clinicians and Doctors with the capacity to make Wise Clinical Decisions – Even before concentrate the patient a specialist can be able to think about the patient and the medicinal profile ordered by breaking down colossal informational collections alongside the patients' own. This can help the specialist in making educated clinical choices remembering the forecasts gave on profound investigation of medicinal services information. Extortion Analysis – Healthcare claims and the related information can be broke down by a Big Data System and expectations can be given on potential fake claims in the Healthcare Protection Sector. This can enable Health to mind protection organizations spare significant cash lost to false claims. In the process medicinal services suppliers who are a piece of extortion can likewise be recognized and proper lawful activity guaranteed. Research – Big information investigation on genomic research and ongoing PHR get to could furnish therapeutic professionals with educated choices and help in treatment. Consistent research will come about in proactive strides being taken before issues happen, opposite to the responsive course of treatment set up today.

VPH or Virtual Physiological Human is a developing structure of techniques and advances for community examination of the human body as a solitary complex framework. Scientific models for foreseeing the condition of an organic framework can be utilized along with medicinal imaging and detecting advances. High dimensional huge information examination has encouraged this exploration and enormous information advances have engaged and fortified VPHapproaches.

II. Healthcare Security and Privacy

Medicinal services Data in Big Data Environments today confront a few difficulties:-

- Sharing of Healthcare information can be utilized by cloud advancements. Social insurance information from various sellers can be converted to examine experiences into medicinal Treatment and analysis. Sharing the information by means of cloud based conditions brings worries up in situations where security rehearses identified with medicinal services are not input.
- Healthcare server farms today are required to take after HIPAA confirmation and the rules and guidelines laid out by HIPAA. This however does not ensure persistent record wellbeing as HIPAA does not lay out standards for actualizing information security but instead is concerned with guaranteeing that security approaches and systems are set up. Additionally, inflow of huge volume of information from different sources brings about necessity of taking care of the additional weight for capacity, handling force and high speed organizing.
- Healthcare industry has confronted a scope of assaults like DDOS (Distributed Denial of Service), malware assaults and Medical Identity Theft by insiders and outer assailants too. Medicinal services information as EHRs or PHRs are private to the individual or the associations managing them. Presentation of medicinal services information and the recognizable proof of an individual can lead to a few concerns.
- Medical Identity Theft – Medical Identity Theft is the most regular type of protection break in Health Care where a person's close to home data is uncovered what's more, from that point mimicked for monetary benefit.
- Social Issues – Exposed wellbeing states of an individual may prompt undesirable social circumstances.

- Insurance Fraud – Fictitious doctor's visit expenses can be gotten on the premise of stolen personality and protection cases can be submitted for monetary benefit.
- Incorrect treatment – if the medicinal data is adjusted in an undesirable way, it might prompt inaccurate treatment of the patient.
- Incorrect Diagnosis – Incorrect medicinal data may prompt mistaken finding or improper treatment design, conceivably hurting the patient's wellbeing. Medical coverage medicines may get depleted and patients will be unable to assert assist protection. Work Issues – Employers do ask for the medicinal history of potential workers and harmed or, then again distorted therapeutic data have the capability of causing work issues. Persistent Data Privacy is of most extreme significance and is basic that appropriate security rehearses are executed and drilled. In this paper some current and proposed methods are examined.

III. BIG DATA SECURITY APPROACHES IN HEALTHCARE

A. Health Care Big Data and Internet of Things

Wireless Body Area Networks or WBANs are used for monitoring of medical condition of patients using tiny sensor nodes attached or implanted to the human body. These sensor nodes develop what is called a Wireless Sensor Network (WSN). Biological information from the human body is sent to a control device either attached to the human body or in the vicinity wirelessly. The collected data is sent to remote servers or cloud of a hospital/medical center for further analysis or action. WBANs can be used for ECG, pulse rate, blood pressure, blood flow, body temperature, EEG etc. It is vital to ensure accuracy and integrity of such healthcare data and hence security and privacy of WBANs must be
Ensured. Security must be maintained for WBANs in: the sensors attached to the body, remote servers where WBAN data is pushed, communication channels. A lot of research has been done on securing WBANs.

- F.A. Khan et al proposed a cloud based healthcare framework for implementing WBANs using cloud computing, wherein patient data stored on the cloud is protected using dynamic reconstruction of metadata. Combination of biometric values is used to generate keys for encryption, thus ensuring randomness.
- Han et al proposed another scheme for data Confidentiality for cloud based WBANs wherein they suggested a cryptosystem having multi valued and ambiguous properties . This was achieved using multi valued encoding rules. In addition, the data communication between the cloud and WBANs is attempted to secure efficiently.

B. Health Care Big Data and Cloud

Cloud computing today is used extensively for Health Information Systems and processing of healthcare data .Advances in Omits fields (genomics, proteomics and meta bionomics) aims in collecting and characterizing pools of biological molecules and their structure, function and dynamics. This generates considerable amount of data to be stored and processed. Predictive analytics using text and data mining algorithms requires a growing demand for dynamic and scalable resources which the cloud computing environment is able to provide. An additional benefit of the cloud computing environment is that resources can be used temporarily as required on a Pay as you use basis with the ability of buying processing power and storage on-demand. Cloud computing is also using for biomedical information sharing.

Cloud computing along with Big Data technologies has found use in Medical Imaging, public health and patients' self-service applications, hospital management and Clinical Information Systems. It is imperative that with the growing use of cloud computing technologies in healthcare, security and privacy of healthcare data in the cloud needs to be preserved along with securing the cloud computing infrastructure itself.

- Xiao et al introduced the concept of Accountable Map Reduce wherein each node is held accountable for their behavior. A group of auditor nodes perform accountability tests (A-tests) which check each node and identify malicious nodes in real time. This framework is applicable to Map Reduce solutions on the cloud and hence can help secure health care data processing.
- Samantha et al in their paper on "k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data "proposed methodology to run data mining classification algorithms on encrypted data. This is relevant for Healthcare data mining on the cloud or for health care data outsourced for mining, wherein the data has to be in encrypted form to ensure privacy and traditional privacy preserving techniques do not apply. To illustrate Data Mining over encrypted data (DMED) secure k-N classifier was used which has been termed as PPk NN or Privacy Preserving k-NN.
- Using Attribute Based Encryption, Yang et al. Proposed an outsourced policy updating method for Big Data Systems in the cloud .

- A Sticky Policy Framework was proposed by Liet al. which suggested an implementation independent meta-model for security policies. A loose-couple binding approach is suggested where data fragments are stored separately from sticky policies. This allows definition of fine-grained security access. Fine grained security access may be used to define different levels of access group's access to only what they need to see e.g. patient data can be accessible only to doctors and nurses only. Inside the patient data, some information may be for the eyes of doctors only.

- Waziri et al. have used fully homomorphism encryption to suggest a cryptographic model for Big Data Analytics in the cloud thereby addressing concerns on Confidentiality and Privacy. Techniques for implementation and concepts on cryptographic solutions for Big Data in the cloud have been discussed.

C. Securing Patient Health Records in Big Data and Cloud Environments

Health care today revolves around the data presented by Electronic Health Records (EHR) which integrates all health related aspects and findings of an individual. Because of the sensitive nature of this information and its potential to cause harm if disclosed, EHRs (or PHRs - Patient Health Records),should be access controlled and strict security and privacy enforced in maintenance. Since health records need to be transferred via internet, stored in the cloud, exposed to vendors, and made part of data analytics they need to be privacy controlled to secure the identity of the individual. While transferring over the internet, transmission encryption is not considered sufficient and the need arises to encrypt the documents as well to protect from hackers and unauthorized access.

- Slamanig et al. in their paper have suggested unlink ability and anonymity as the preliminary criteria in health care data privacy. Unlink ability denotes that relation between data existing in the system should not be identifiable by mere observation. Anonymity is the state of not being identifiable within a set of items which have been defined as the anonymity set. The paper also discusses the dangers of utilizing plaintext entryways which store information without encryption and thus are powerless against assaults from insiders and programmers. For encoded entryways, which scramble the wellbeing information it is critical to secure the cryptographic key on the servers as insiders might have the capacity to access it. This should be possible by utilizing a Public Key Infrastructure (PKI) and is scrambled utilizing the general population key of the individual to whom get to is allowed. Also, pseudonym zed entrances can be utilized wherein encryption is accomplished for the substance and the meta-information too. Wellbeing records are additionally subject to revelation in cases EHRs are presented to a few gatherings of individuals e.g. potential businesses, insurance agencies and so on.

- Gunamalai et al. propose a technique for security and protection of Personal Medical Records and DICOM pictures in the Cloud condition [21]. DICOM (Digital Imaging and Communication in Medicine) is a standard for restorative imaging and furthermore tends to dissemination and review of therapeutic pictures. The objective is to empower various social insurance focuses to get to patients' information for treatment secury. The plan imperceptibly installs private patient information like name and extraordinary recognizable proof number in the restorative pictures. Get to Control is done by means of two-way verification which is a blend of username secret key approval and a dynamic key sent to a handheld gadget or email. To secure information in the cloud servers, Column Based Encryption (CBE) is utilized which empowers specific sharing of information among human services focuses.

- E. Srimathi et al propose a technique for guaranteeing protection of medicinal services records in Big Data utilizing Dynamic Map Reduce. Their work is identified with giving anonymizing methods to securing adaptable Big Data. They utilize a two-stage approach utilizing Dynamic Map Reduce structure and the LKC security show . Dynamic Map Reduce is an idea empowering dynamic assignment of sit still openings with no running undertakings. This advancement includes 2 procedures to be specific: Dynamic Hadoop Slot Allocation (DHSA) – Unused guide or decrease openings can be utilized conversely to enhance execution. Theoretical Execution Performance Balancing (SEPB) – Speculative execution is utilized to distinguish slacking errands. The LKC protection show includes l-assorted variety to avoid connecting Quasi Identifier (QID) traits for re-ID.

D. Health Care and Big Data Analytics

A strong basic leadership framework in the medicinal services industry requires sharing of Electronic Health Records as well as of running prescient calculations to distinguish slants in treatment, conclusion and other research zones. The principle impediments in sharing the EHRs are tolerant protection and the affectability of therapeutic data contained in them.

- Yan Li et al. proposed a conveyed (group of appropriation of irregular factors) approach for mining human services information under protection requirements [24]. Each taking an interest office getting to the information needs to construct their own model to take in the dissemination

of their own information. From that point they share the learning obtained information on their information as choice models. Subsequently the patient level delicate information is not shared hence safeguarding protection.

- Noman Mohammed et al. in their paper on Secure and private administration of human services databases for information mining [25] recommended a system which employments "semantically-secure" encryption plans to scramble information bases being outsourced. Their system empowers questioning the information utilizing a "differentially-private" inquiry interface supporting SQL inquiries and complex information mining errands. Systematic preparing done on information ought not uncover individual information for clients or granular points of interest that would lead examiners to follow back the information to the first subtle elements. Information mining and prescient examination strategies need to actualize security safeguarding methods e.g. concealing touchy information and other anonymization systems. Protection Preserving Data Mining and Analytics is a system investigated today by numerous analysts to fathom this issue.

- Agrawal et al proposed an approach identified with Privacy Preserving Data digging for building classifiers utilizing preparing information [26]. The information on which classifiers are fabricated are not same as the first, while being unique in relation to the first in dispersion and qualities. A novel remaking method was proposed to appraise the conveyance of unique information from the preparation information gave. Classifiers for the information mining can be assembled utilizing this and the precision of these classifiers were appeared to be tantamount to classifiers fabricated utilizing the genuine

  information. Since the real information is not used to manufacture classifiers for this situation, security of delicate client data can be safeguarded. The essential approach is to give clients a chance to give information arbitrary commotion added to it. 2 strategies for changing esteems are considered – by discretizing esteems into totally unrelated classes and by adjusting esteems utilizing a component of arbitrary esteems with uniform or Gaussian dissemination. Lindell et al proposed an approach on Privacy Preserving Data Mining considering 2 parties endeavoring to run information mining with a union of their particular databases. The aim was to not uncover pointless data. They utilized choice tree learning and the ID3 calculation to propose an effective approach. No gathering required here adapted more than the yield itself.

- Quasi-identifiers are properties that can be utilized to particularly recognize people by connecting to outer information. To counter this security issue the idea of k-anonimity [28] was presented. In this technique information is summed up or smothered to diminish granularity. In the event that a record k in a dataset is unclear from in any event k − 1 different records concerning each arrangement of semi identifier characteristics, the dataset can be called k-unknown. It was appeared however that k-anonimity is not trick verification with regards to information security as it can be subjected to assaults like "Homogeneity assault" when there is Homogeneity of delicate qualities and "Foundation information assault" wherein foundation learning on the individual is useful in distinguishing proof. A. Machanavajjhala et al. recommended l-diversity[29] to secure against the protection issues that might be experienced when utilizing k-obscurity. To do as such, the idea of intra-amass decent variety of touchy esteems is advanced inside the anonymization scheme[30].

- Reza Shokri et al. In their paper on Privacy safeguarding profound learning examined about a structure to protect security of client information in profound learning neural systems. Their framework empowers 2 gatherings to mutually learn neural system models without uncovering the first datasets. This was accomplished by sharing of chose display parameters amid preparing. As indicated in the paper – "this parameter sharing, interleaved with neighborhood parameter refreshes amid stochastic inclination drop, enables members to profit by other members' models without express sharing of preparing inputs" .

IV. CONCLUSION

While Big Data advancements are enhancing step by step this likewise implies the volume of information alongside the rate at which information is streaming into endeavors today is expanding. There is a need to secure touchy medicinal services information from foes and pernicious programming – both to keep up honesty of the information and protection of delicate data. The security challenges featured should hence be managed and new novel security approaches need to come up that can be adjusted to Health Care Big Data. While programming security goes long back in calculation history, not all strategies are reasonable in the medicinal services setting. The achievement of security strategies in ensuring information and the capacity of sharing information without protection concerns will decide the capability of Health Care Data adjustment to cloud based conditions in the coming d

V. APPENDIX A – HEALTHCARE ACTS

Country	Healthcare Act	Description
US	Medicare	National social protection program in the US controlled by the US government. Gives medical coverage to Americans matured 65 or more, and to individuals of all more youthful age with a few incapacities.
	HIPAA	The Health Insurance Portability What's more, accountability Act of 1996 (HIPAA). Incorporates rules for discharging and sharing exclusively identifiable data which are some portion of electronic well being records. A patient's medicinal record can't be legitimately unveiled without the composed approval of the patient. Every single medicinal supplier and others trying to get to or keeping up well being records in the US should be HIPAA consistent. The privacy Rule of HIPAA addresses the utilization and revelation of a patient's ensured well being data by medicinal services designs, medicinal suppliers, and Clearinghouses, likewise alluded as secured elements. The security rule of HIPAA requires secured elements to guarantee execution of managerial defends in the type of approaches and staff, physical protections to data foundation, and specialized shields to screen and control intra and bury hierarchical data get to.

VI. APPENDIX B - HEALTHCARE TERMINOLOGIES

Phrasing	Description
EHR	A digitized variant of the patient's medicinal record. An HER can contain a patient's restorative history, analyze, solutions, treatment designs, vaccination dates, hypersensitivities, radiology pictures, what's more, research facility and test outcomes and furthermore permit access to confirm based apparatuses that suppliers can use to settle on choices about a patient's care.
PHR	PHRs contain comparable data as EHRS with the expansion that PHRs are expected to engage patients, and to furnish them with the capacity to check their records for any irregularities and restorative mistakes paying little respect to area.

REFERENCES

[1]. J. D. Halamka, "Using Big Data to Make Wiser Medical Decisions," Harvard Business Review, 2015. [Online]. Available: https://hbr.org/2015/12/using-big-data-to-make-wiser-medical-decisions.
[2]. B. Marr, "How Big Data Is Changing Healthcare," Forbes, 2015. [Online]. Available: http://onforb.es/1bfRQ0b.
[3]. M. Viceconti, P. Hunter, and R. Hose, "Big Data , Big Knowledge : Big Data for Personalized Healthcare," IEEE Journal of Biomedical and Health Informatics, vol. 19, no. 4, pp. 1209–1215, Jul. 2015.
[4]. H. Kupwade Patil and R. Seshadri, "Big Data Security and Privacy Issues in Healthcare," in 2014 IEEE International Congress on Big Data, 2014, pp. 762–765.
[5]. W. C. Figg and H. J. Kam, "Medical Information Security," International Journal of Security, vol. 5, no. 1, pp. 22–34, 2011.
[6]. E. Srimathi and K. A. Apoorva, "Preserving Identity Privacy of Healthcare Records in Big Data Publishing Using Dynamic MR," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 4, pp. 968–973, 2015.
[7]. W. Gillette and T. B. Patrick, "Medical identity theft: an emerging problem for informatics.," AMIA Annual Symposium proceedings AMIA Symposium AMIA Symposium, p. 964, 2007.
[8]. J. Y. Khan and M. R. Yuce, "Wireless Body Area Network (WBAN) for Medical Applications," in New Developments in Biomedical Engineering, Online Edi., InTech, 2010, pp. 591– 628.
[9]. A. Tewari, "Security and Privacy in E-Healthcare Monitoring with WBAN : A Critical Review," International Journal of Computer Applications, vol. 136, no. 11, pp. 37–42, 2016.
[10]. F. A. Khan, A. Ali, H. Abbas, and N. A. H. Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks," Procedia Computer Science, vol. 34, pp. 511–517, 2014.
[11]. A. Waqar, A. Raza, H. Abbas, and M. Khurram Khan, "A framework for preservation of cloud users data privacy using dynamic reconstruction of metadata," Journal of Network andComputer Applications, vol. 36, no. 1, pp. 235–248, 2013.
[12]. N. D. Han, L. Han, D. M. Tuan, H. P. In, and M. Jo, "A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks," Information Sciences, vol. 284, pp. 157–166, 2014.
[13]. L. Griebel, H.-U. Prokosch, F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, "A scoping review of cloud computing in healthcare.," BMC medical informatics and decision making, vol. 15, p. 17, 2015.
[14]. Z. Xiao and Y. Xiao, "Achieving Accountable MapReduce in cloud computing," Future Generation Computer Systems, vol. 30, pp. 1–13, 2014.
[15]. H. Ulusoy, M. Kantarcioglu, E. Pattuk, and L. Kagal,"AccountableMR: Toward accountable MapReduce systems," in 2015 IEEE International Conference on Big Data (Big Data), 2015, pp. 451–460.
[16]. B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "K-nearest neighbor classification over semantically secure encrypted relational data," IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 5, pp. 1261–1273, 2015.
[17]. K. Yang, X. Jia, and K. Ren, "Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud,"IEEE Transactions on Parallel and Distributed Systems, vol. PP, no. 99, pp. 1–1, 2014.
[18]. J. Gao, S. Li, T. Zhang, J. Gao, and Y. Park, "A Sticky Policy Framework for Big Data Security," no. October, pp. 130–137, 2015.
[19]. V. O. Waziri, J. K. Alhassan, I. Ismaila, and M. N. Dogonyaro, "Big Data Analytics and Data Security in the Cloud via Fully Homomorphic Encryption," International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 9, no. 3, pp. 744–753, 2015.
[20]. D. Slamanig and C. Stingl, "Privacy aspects of eHealth," in ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings, 2008, pp. 1226–1233.
[21]. C. Gunamalai and S. Sivasubramanian, "A Novel Method Of Security And Privacy For Personal Medical Record And Dicom Images In Cloud Computing," ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 10, pp. 4635–4638, 2015.
[22]. S. Tang, B. S. Lee, and B. He, "DynamicMR: A dynamic slot allocation optimization framework for mapreduce clusters," IEEE Transactions on Cloud Computing, vol. 2, no. 3, pp. 333– 347, 2014.
[23]. N. Mohammed, B. C. M. Fung, P. C. K. Hung, and C.-K. Lee, "Centralized and Distributed Anonymization for High-Dimensional Healthcare Data," ACM Transactions on Knowledge Discovery from Data, vol. 4, no. 4, pp. 1–33, 2010.
[24]. Y. Li, C. Bai, and C. K. Reddy, "A distributed ensemble approach for mining healthcare data under privacy constraints," Information Sciences, vol. 330, no. 330, pp. 245–259, 2015.
[25]. N. Mohammed, S. Barouti, D. Alhadidi, and R. Chen, "Secure and private management of healthcare databases for data mining," in Proceedings - IEEE Symposium on Computer-Based Medical Systems, 2015, vol. 2015-July, pp. 191–196.
[26]. R. Agrawal and R. Srikant, "Privacy-preserving data mining,"Proceedings of the 2000 ACM SIGMOD international conference on Management of data - SIGMOD '00, vol. 29, no. 2, pp. 439–450, 2000.

[27]. Y. Lindell and B. Pinkas, “Privacy-preserving Data Mining,” Crypto ’00, vol. 29, pp. 36–54, 2000.
[28]. P. Samarati and L. Sweeney, “Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement Through Generalization and Suppresion.,” Proc of the IEEE Symposium on Research in Security and Privacy, pp. 384–393, 1998.
[29]. A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, “L -diversity,” ACM Transactions onKnowledge Discovery from Data, vol. 1, no. 1, p. 3–es, 2007.
[30]. C. C. Aggarwal and P. S. Yu, “A General Survey of Privacy-Preserving Data Mining Models and Algorithms,” in Privacy-preserving data mining, Springer US, 2008, pp. 11–52.
[31]. R. Shokri and V. Shmatikov, “Privacy-Preserving Deep Learning,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS ’15, pp. 1310–1321, 2015.
[32]. A. Appari and M. E. Johnson, “Information security and privacy in healthcare: current state of research,” International Journal of Internet and Enterprise Management, vol. 6, no. 4, p. 279, 2010.
[33]. “Patient Protection and Affordable Care Act,” Wikipedia.[Online]. [Accessed: 20-Aug-2016].