International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 283-294
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

BIG DATA PRIVACY IN BIOMEDICAL RESEARCH

C. Seetha Lakshmi[1], Mr.S.Kannan[2], Dr.A.Muthukumaravel [3]
[1] Mphil. CS-Research Scholar, Department of MCA, BIHER, Chennai, Tamil Nadu, India
[2] Assistant professor, Department of MCA, BIHER, Chennai, Tamil Nadu, India
[3] Dean-Faculty of Arts & Science, & HOD-Department of MCA, BIHER, Chennai, Tamil Nadu, India

In this project, we aim at developing big data solutions for classifying encrypted large-volume, complex, growing data sets with multiple, autonomous sources.

If properly analyzed, the patterns could be a source of rich intelligence for classifying service usages. Furthermore, from the security and privacy perspective, the underlying issue we leverage is that current privacy protection technology conceals the content of patient details, while they do not prevent the detection of data network patterns that instead may reveal some sensitive information about the user's preference and behaviour.

We analyze the each and every data set sensitive field and give priority for this sensitive field. Then we apply ANONYMIZATION on this sensitive field only depending upon the scheduling. Specifically, privacy methods have been developed to protect against various attack models. This paper reviews relevant topics in the context of biomedical research.

In addition, we learn a service usage predictor by feeding the extracted features and the reported usage types into the chosen classifiers. Moreover, for those outlier dialogs with mixed usage, we exploit a clustering method to further regment these dialogs into sub dialogs.

We selected a few important and practical topics in biomedical research to discuss related privacy preserving technologies. These topics include: record linkage, distributed data analysis, synthetic data generation, and secure genome analyses.

We will focus on both privacy protection technologies for both electronic health records (EHR) and genomic data.

Keywords: *EHA, anonymization, big data.*

1. INTRODUCTION

Big data is data sets that are so voluminous and complex that traditional data processing application software are inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating and information privacy. In the big data environment, anonymity protection is necessary to protect the data. For example, in social networks, anonymity protection can be divided into user identity anonymity, attributes anonymity and relationship anonymity (known as edge anonymity). The information of user identification and user attribute must be hidden when published; the relationship anonymity is to hide the relationship between users when data is released. At present, the relationship anonymity is a hotspot of research, many scholars have studied multiple methods for the relationship anonymity. Through other public information, an attacker may be inferring anonymous users, especially relationship between the users. The outcomes of the competitions identified several limitations in the current genome privacy protection studies. First, genomic data protection using perturbation-based protection methods often present too much noise, where practical genomic applications may not be able to trustworthily rely on these noise outputs. Second, cryptography-based protection methods for secure collaboration or outsourcing currently only support limited genomic computations due to their complexity. Third, the ethical implications of these protection methods are not yet clear. Therefore, further investigations of genome privacy are important and necessary, which motivates researchers to develop advanced genome privacy protection technologies and to investigate their ethical implications. We discuss privacy preserving technologies related to (1) record linkage, (2) synthetic data generation, and (3) genomic data privacy. We also discuss the ethical implications of big data privacy in biomedicine and present challenges in future research directions for improving data privacy in biomedical research.

2. PATIENT DETAILS, MEDICAL NETWORK AND BIG DATA

The current privacy-enhancing technologies for genomic data are susceptible to compromise. Specifically, this work studies computational attacks that leverage information learned from shared genomic data and additional resources for linkage to named individuals. None of the systems analyzed is impregnable to re-identification. Rather, there exist patterns of flaws due to neglect of inferences that can be made from genomic data itself and the environments in which the data are shared. With the increasing needs of keeping and linking electronic patient records, it is very challenging to maintain security and preserve privacy.

Under the regulations of the Health Insurance Portability and Accountability Act (HIPAA), preserving patient's privacy is important in linking the patient's data. As medical databases contain different identifiers of a patient (eg, patient's name, surname, date of birth, Social Security Number-SSN, contact number, address, etc), using these identifiers in their actual form for linking purpose violates privacy.

[1]

However, when we consider the real life scenario, it is possible that existing works might not meet all the requirements of medical record linkage all the time in practice. For instance, earlier researches on data record linkage (ie, sending identifiers in encrypted format does not allow any kind of error in identifiers) may happen frequently in real cases. Spelling mistakes and typographical errors are very common in databases. Privacy preserving error-tolerant linkage guarantees that computing the error-tolerant linkage function is secure in the semi honest model, without a trusted third party.

[2]

By secure encapsulation and publishing of bioinformatics software in a big data environment, while they worked on only biological services and focused on achieving a prototype system of the biological data, our solution works on different databases and concentrates on linking these different databases in a privacy preserving manner. The proposed algorithm considers health data containing both relational and set-valued data and accomplishes "element-of" differential privacy. [3] In our solution, instead of different categories of medical data and heterogeneous health data, we concentrate on textual and numeric data and further categorize them into error-free data and error-prone data. . The proposed solution decouples the data, obfuscates it, and shares minimum information via encryption, chaffing, and recoding respectively, to ensure the protection against attribute disclosure. A new computer-based third party record linkage platform has been proposed in database, but our proposed solution does not need a trusted third party [4]-[6].

For working on these massively distributed peta bytes of medical network data, we will use the human genome research, one of the most promising medical and health areas as an example and application of Big Data science, is discussed to demonstrate how the adaptive advanced computational analytical tools could be utilized for transforming millions of data points into predictions and diagnostics for precision medicine and personalized healthcare with better patient outcomes.

Hadoop framework that is a practical approach to self-describing, polymorphic, and parallelizable user defined functions. This feature improves large data sets through parallelized execution and makes it possible to test the algorithm with substantial volumes of data about users, devices, and activities. They use programming language such as Java, C or C++.

3. BIO-MEDICAL ANALYSIS FOR RESEARCH AND PRESERVING DATA

To enhance the health care quality and public health surveillance, privacy preserving medical record linkage among different medical service providers is very important. As the real-world medical record may well be error-prone, the goal of our study was to design and develop a software system that helps medical record linkage for both error-free data and error-prone data, and preserves privacy too. We have successfully designed a comprehensive system to achieve this goal. Moreover, our software meets the regulation of HIPAA and does not require a trusted third party. Our software preserves privacy since no party can get to know about another’s database. As the existing works on error-prone data are limited to textual data, we propose a novel algorithm named the Error-Tolerant Linking Algorithm, which works on error-prone numeric data. We offer two cryptographic schemes, the SHA-1 and SHA-2 for error-free data. We designed our software open and each cryptographic scheme is independent to each other so that any existing work/cryptographic scheme for error-prone textual data can be integrated later.

In clinical practice, disease characterization is routinely collected from a number of different streams, such as imaging, pathology, genomics, and electrophysiology. However, much of the deeper insights into disease processes and mechanisms remain to be uncovered and interpreted from routinely acquired clinical data. Clinical data of millions of patients at a clinic/hospital or in a large study exhibit many of the features of Big Data.

The volume comes from large amounts of records that can be derived from the EHRs for patients; for example, medical images including magnetic resonance imaging (MRI) or neuroimaging data for each patient can be large, while social media data gathered from a population can be large-scale as well.

With the popularity of electronic patient records and the expanded use of medical information systems, nowadays many different health care providers store medical records of patients electronically. In many cases different health care providers hold the same patient's data. To enhance the quality of health care treatment, for example, in regional health information networks, often it is required to gather information about the same patient from different providers.

In order to identify whether a particular patient's information is held by more than one health care provider or not, a matching technique is used on the key attributes of the patient's demographic information. As another example, public health surveillance often requires linking patient records from different health care providers.

To encrypt the data, the initiated organization chooses a dataset name and the cryptographic scheme, and sends both of them to the participating organization. If the participating organization holds the same dataset, it starts the privacy preserving data linkage process by sending the data in cipher text format to the initiated organization. Meanwhile, the initiated organization encrypts its own dataset by using the cryptographic scheme. After receiving the data, the initiated organization applies the privacy preserving matching scheme to obtain the results.

. The human genome research, one of the most promising medical and health areas as an example and application of Big Data science, is discussed to demonstrate how the adaptive advanced computational analytical tools could be utilized for transforming millions of data points into predictions and diagnostics for precision medicine and personalized healthcare with better patient outcomes.

4. Record Linkage

Record linkage is used most frequently to create master files for populations or to extend record-level information in one data set with information from another. In hot spotting, record linkage is used to link patient information across different hospitals so that ED and inpatient use can be analyzed.

Record linkage is highly sensitive to the quality of the data being linked, so all data sets under consideration (particularly their key identifier fields) should ideally undergo a data quality assessment prior to record linkage. Many key identifiers for the same entity can be presented quite differently between data sets, which can greatly complicate record linkage unless understood ahead of time.

To linking the data from two different organizations, the Error-Tolerant Linking Algorithm preserves privacy as well. We assume that the attributes of records are preprocessed and converted to integers beforehand.

For numerical attributes, this preprocessing is straightforward by normalizing the original values to integers within a certain range. For attributes consisting of strings, we can use a preprocessing method to convert the strings into integers so that the integers can still keep the distance between the records. Then our algorithm can be applied afterwards to complete the records linkage. This algorithm allows the input record with minor deviations less than a small threshold τ. The threshold value is to calculate the distance between the identifiers of two records. In this algorithm, neither entity can learn the records of each other's patients.

5. WHY HADOOP?

Apache Hadoop may be a distributed system for process giant amounts of knowledge. in an exceedingly recent Hadoop Summit 2010 Yahoo, Facebook, and different corporations declared that they presently method many TBs of knowledge per day and also the volumes area unit growing at exponential rates. Hadoop is very important for finding the fraud detection drawback because:

- ➢ Sampling doesn't work for rare events since the possibility of missing a fraud in fact case ends up in important deterioration of model quality.
- ➢ Hadoop will solve abundant tougher issues by leverage multiple cores across thousands of machines and search through abundant larger drawback domains.
- ➢ Hadoop is combined with different tools to manage moderate to low response latency needs.

Let's bear these reasons one by one. Sampling may be a common technique for modeling rare events. one amongst the issues with sampling is that we tend to cannot afford to throw away rare positive cases. Even in an exceedingly stratified or sampling theme one needs to retain all positive cases since the model accuracy heavily depends on them (one will typically discard some negative cases though). Given the on top of, the system still needs to bear the total dataset to sieve through the positive and negative cases.

Hadoop is understood for its gnawing power. Nothing will compare with the output power of thousands of machines every of that has multiple cores. As was according recently at the Hadoop Summit 2010, the most important installations of Hadoop have two,000 to 4,000 computers with eight to twelve cores every, amounting to up to forty eight,000 active threads yearning for a pattern at constant time. this enables either (a) searching through larger periods of your time to include events across a bigger timeframe or (b) taking additional sources of data under consideration. it's quite common among social network corporations to comb through twitter blogs in search of relevant knowledge.

Finally, one amongst the fraud interference issues is latency. The agencies wish to react to an occurrence as shortly as attainable, typically inside many minutes of the event. Yahoo recently according that it will alter its activity model in an exceedingly response to a user click event inside 5-7 minutes across many hundred of innumerable customers and billions of events per day. Cloud era has developed a tool, Flume, which will load billions of events into HDFS inside many seconds and analyze them victimization MapReduce.

Often fraud detection is like “finding a needle in an exceedingly haystack”. One needs to bear mountains of relevant and on the face of it unsuitable info, build dependency models, appraise the impact and thwart the fraudster actions. Hadoop helps with finding patterns by process mountains of data on thousands of cores in an exceedingly comparatively short quantity of your time.

6. SHA and Error-Tolerant

We introduce SHA and Error-Tolerant, a new, generic, scalable, and integrated approach on however (Biomedical) network analytics will improve the performance on data.

SHA provide security and to identify revisions and to ensure that the data has not changed due to accidental corruption.

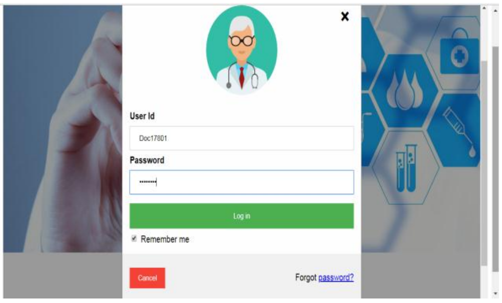
Human error is frequently judged to be a primary contributor to high-consequence accidents in complex systems. This chapter explores this issue and argues that total elimination of human error is a futile pursuit. Instead, systems should be designed so that they are error tolerant in the sense that errors can occur without leading to unacceptable consequences. The idea of error tolerance is described in terms of its empirical basis and an evolving conceptual architecture for error tolerant interfaces.

It is seldom possible to completely prescribe human behaviour and eliminate all possibilities for deviations. When it is possible, it is likely that automation is feasible and, therefore, human performance need not be an element of the system.

7. RESULT AND ANALYSIS

By using the above logic, we studied the execution of Big data privacy in Biomedical Research. Here depending upon the SHA and error tolerant method the protect the patient personal medical data. So that the data can be protect from the unknown user and other things. The results obtained are below

Fig 1: Home Page


User Id

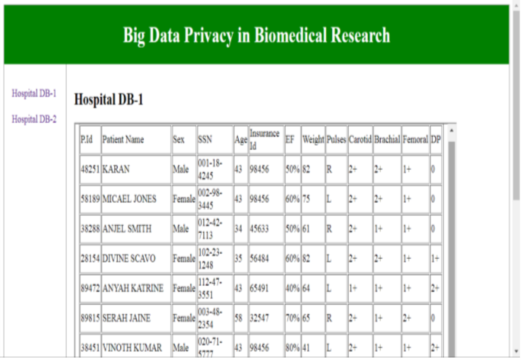
Doc17801

Password

•••••••|

✓ Remember me

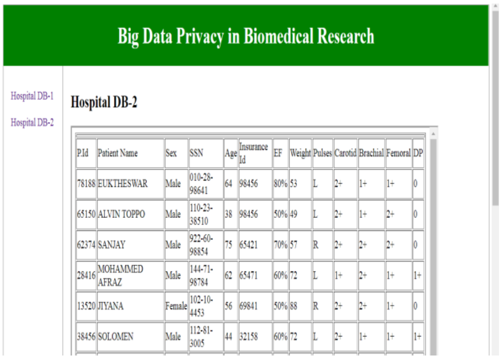
Fig 2: Login Page



Hospital DB-1

P.Id	Patient Name	Sex	SSN	Age	Insurance Id	EF	Weight	Pulses	Carotid	Brachial	Femoral	DP
48251	KARAN	Male	001-18-4245	43	98456	50%	82	R	2+	2+	1+	0
58189	MICAEL JONES	Female	002-98-3445	43	98456	60%	75	L	2+	2+	1+	0
38288	ANJEL SMITH	Male	012-42-7113	34	45633	50%	61	R	2+	1+	1+	0
28154	DIVINE SCAVO	Female	102-23-1248	35	56484	60%	82	L	2+	2+	1+	1+
89472	ANYAH KATRINE	Female	112-47-3551	43	65491	40%	64	L	1+	1+	1+	2+
89815	SERAH JAINE	Female	003-48-2354	58	32547	70%	65	R	2+	1+	2+	0
38451	VINOTH KUMAR	Male	020-71-5777	43	98456	80%	41	L	2+	1+	1+	2+

Fig 3: Record linkage database 1

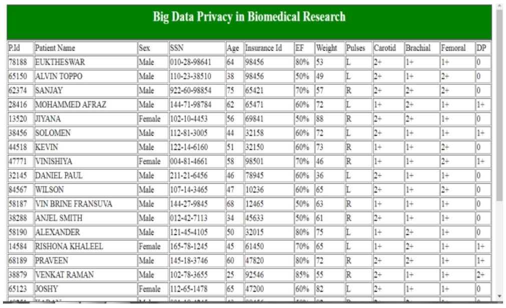


Big Data Privacy in Biomedical Research

Hospital DB-2

P.Id	Patient Name	Sex	SSN	Age	Insurance Id	EF	Weight	Pulses	Carotid	Brachial	Femoral	DP
78188	EUKTHESWAR	Male	010-28-98641	64	98456	80%	53	L	2+	1+	1+	0
65150	ALVIN TOPPO	Male	110-23-38510	38	98456	50%	49	L	2+	1+	2+	0
62374	SANJAY	Male	922-60-98854	75	65421	70%	57	R	2+	2+	2+	0
28416	MOHAMMED AFRAZ	Male	144-71-98784	62	65471	60%	72	L	1+	2+	1+	1+
13520	JIYANA	Female	102-10-4453	56	69841	50%	88	R	2+	2+	1+	0
38456	SOLOMEN	Male	112-81-3005	44	32158	60%	72	L	2+	1+	1+	1+

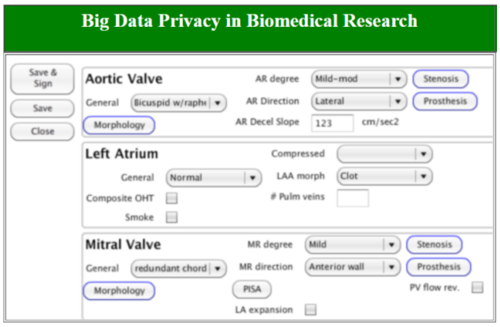
Fig 3: Record linkage database 2



Big Data Privacy in Biomedical Research

P.Id	Patient Name	Sex	SSN	Age	Insurance Id	EF	Weight	Pulses	Carotid	Brachial	Femoral	DP
78188	EUKTHESWAR	Male	010-28-98641	64	98456	80%	53	L	2+	1+	1+	0
65150	ALVIN TOPPO	Male	110-23-38510	38	98456	50%	49	L	2+	1+	2+	0
62374	SANJAY	Male	922-60-98854	75	65421	70%	57	R	2+	2+	2+	0
28416	MOHAMMED AFRAZ	Male	144-71-98784	62	65471	60%	72	L	1+	2+	1+	1+
13520	JIYANA	Female	102-10-4453	56	69841	50%	88	R	2+	2+	1+	0
38456	SOLOMEN	Male	112-81-3005	44	32158	60%	72	L	2+	1+	1+	1+
44518	KEVIN	Male	122-14-6160	51	32150	60%	73	R	1+	1+	2+	0
47771	VINISHIYA	Female	004-81-4661	58	98501	70%	46	R	1+	1+	2+	1+
32145	DANIEL PAUL	Male	211-21-6456	46	78945	60%	36	L	2+	1+	1+	0
84567	WILSON	Male	107-14-3465	47	10236	60%	65	L	2+	1+	2+	0
58187	VIN BRINE FRANSUVA	Male	144-27-9845	68	12465	50%	63	R	1+	1+	1+	0
38288	ANJEL SMITH	Male	012-42-7113	34	45633	50%	61	R	2+	1+	1+	0
58190	ALEXANDER	Male	121-45-4105	50	32015	80%	75	L	1+	2+	1+	0
14584	RISHONA KHALEEL	Female	165-78-1245	45	61450	70%	65	L	1+	2+	1+	1+
68189	PRAVEEN	Male	145-18-3746	60	47820	80%	72	R	2+	2+	1+	1+
38879	VENKAT RAMAN	Male	102-78-3655	25	92546	85%	55	R	2+	1+	1+	2+
65123	JOSHY	Female	112-65-1478	65	47200	60%	82	L	2+	1+	1+	0

Fig 4: Synthetic Data



Big Data Privacy in Biomedical Research

Aortic Valve

General: Bicuspid w/raph

AR degree: Mild-mod

AR Direction: Lateral

AR Decel Slope: 123 cm/sec2

Left Atrium

General: Normal

Compressed:

LAA morph: Clot

Composite OHT □

Smoke □

Pulm veins:

Mitral Valve

General: redundant chord

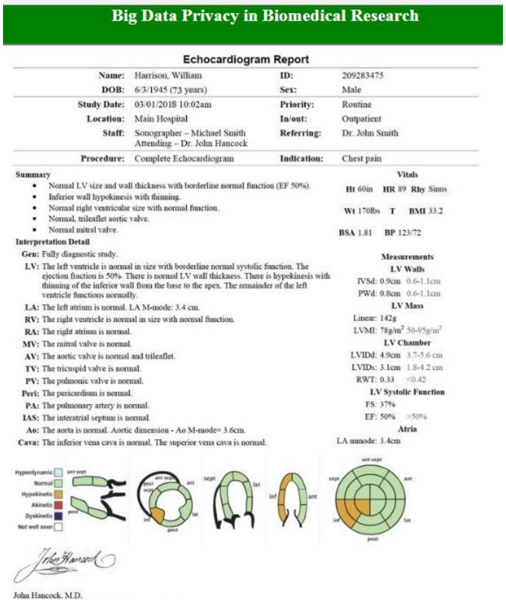
MR degree: Mild

MR direction: Anterior wall

PV flow rev. □

LA expansion □

Fig 5: Patient Medical Details



Big Data Privacy in Biomedical Research

Echocardiogram Report

Name:	Harrison, William	**ID:**	209283475
DOB:	6/3/1945 (73 years)	**Sex:**	Male
Study Date:	03/01/2018 10:02am	**Priority:**	Routine
Location:	Main Hospital	**In/out:**	Outpatient
Staff:	Sonographer – Michael Smith Attending – Dr. John Hancock	**Referring:**	Dr. John Smith
Procedure:	Complete Echocardiogram	**Indication:**	Chest pain

Summary

- Normal LV size and wall thickness with borderline normal function (EF 50%).
- Inferior wall hypokinesis with thinning.
- Normal right ventricular size with normal function.
- Normal, trileaflet aortic valve.
- Normal mitral valve.

Interpretation Detail

Gen: Fully diagnostic study.

LV: The left ventricle is normal in size with borderline normal systolic function. The ejection fraction is 50%. There is normal LV wall thickness. There is hypokinesis with thinning of the inferior wall from the base to the apex. The remainder of the left ventricle functions normally.

LA: The left atrium is normal. LA M-mode: 3.4 cm.

RV: The right ventricle is normal in size with normal function.

RA: The right atrium is normal.

MV: The mitral valve is normal.

AV: The aortic valve is normal and trileaflet.

TV: The tricuspid valve is normal.

PV: The pulmonic valve is normal.

Peri: The pericardium is normal.

PA: The pulmonary artery is normal.

IAS: The interatrial septum is normal.

Ao: The aorta is normal. Aortic dimension - Ao M-mode= 3.6cm.

Cava: The inferior vena cava is normal. The superior vena cava is normal.

Vitals

Ht 60in **HR** 89 **Rhy** Sinus

Wt 170lbs **T** **BMI** 33.2

BSA 1.81 **BP** 123/72

Measurements

LV Walls

IVSd: 0.9cm 0.6-1.1cm

PWd: 0.8cm 0.6-1.1cm

LV Mass

Linear: 142g

LVMI: 78g/m^2 50-95g/m^2

LV Chamber

LVIDd: 4.9cm 3.7-5.6 cm

LVIDs: 3.1cm 1.8-4.2 cm

RWT: 0.33 <0.42

LV Systolic Function

FS: 37%

EF: 50% >50%

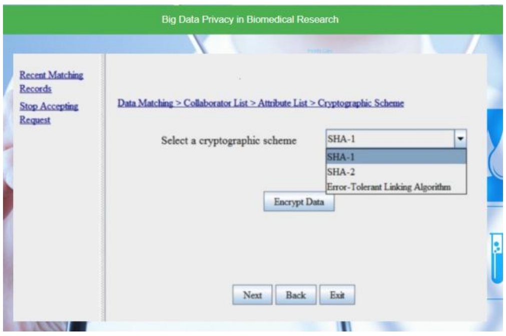
Atria

LA mmode: 3.4cm

John Hancock

John Hancock, M.D.

Fig 6: Patient Medical Report

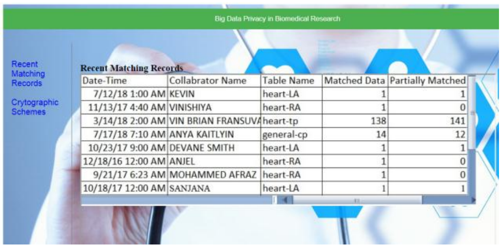


Big Data Privacy in Biomedical Research

Data Matching > Collaborator List > Attribute List > Cryptographic Scheme

Select a cryptographic scheme: SHA-1

Fig 7: Choosing schemas



Big Data Privacy in Biomedical Research

Recent Matching Records

Date-Time	Collabrator Name	Table Name	Matched Data	Partially Matched
7/12/18 1:00 AM	KEVIN	heart-LA	1	1
11/13/17 4:40 AM	VINISHIYA	heart-RA	1	0
3/14/18 2:00 AM	VIN BRIAN FRANSUVA	heart-tp	138	141
7/17/18 7:10 AM	ANYA KAITLYIN	general-cp	14	12
10/23/17 9:00 AM	DEVANE SMITH	heart-LA	1	1
12/18/16 12:00 AM	ANJEL	heart-RA	1	0
9/21/17 6:23 AM	MOHAMMED AFRAZ	heart-RA	1	0
10/18/17 12:00 AM	SANJANA	heart-LA	1	1

Fig 8: Recently Matched Records

6. CONCLUSION

In this paper, we tend to improve the performance of privacy in Biomedical Research. This research provided an analysis of the re-identification susceptibility of genomic data privacy protection methods for shared data. The results prove the current set of privacy protection methods do not guarantee the protection of the identities of the data subjects.

This work stresses that a new direction in the research and advancement of anonymity protection methods for genomic data must be undertaken. The next generation of privacy protection methods must account for both social and computational interactions that occur in complex data sharing environments.

In addition, privacy protection methods must provide proofs about what protections can and cannot be afforded to genomic data, as well as the limits of research with protected data. The development of new identity protection strategies is paramount for continued data sharing and innovative research.

REFERENCES

[1] Brabham DC, Ribisl KM, Kirchner TR, Bernhardt JM. Crowd sourcing applications for public health. American Journal of Preventative Medicine. 2014.

[2] Lissovoy G. Big data meets the electronic medical record: A commentary on identifying patients at increased risk for unplanned readmission. Medical Care. 2013.

[3] Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health Inf Sci Syst. 2014.

[4] Murdoch TB, Detsky AS. The inevitable application of big data to health care. JAMA. 2013.

[5] Dr.R.Kousalya, T.Sindhupriya, “Review on Big Data Analytics and Hadoop Framework”, International Journal of Innovations in Scientific and Engineering Research (IJISER), Vol.4, No.3, pp.78-82, 2017.

[6] Bates D, Saria S, Ohno-Machado L, Shah A, Escobar G. Big data in health care: Using analytics to identify and manage high-risk and high-cost patients. Health Affairs. 2014.

[7] Gardner E. The HIT approach to big data: Everyone in this market is trying to corral their massive data sets. Health Data Management. 2013.

[8] Laney D. 3D Data Management: Controlling Data Volume, Velocity and Variety. Gartner. 2001.

[9] Laney D, Beyer MA. The Importance of ‘Big Data’: A Definition. Gartner. 2012.

[10] Collins FS, Green ED, Guttmacher AE, Guyer MS. A vision for the future of genomics research. Nature. 2003.

[11] McElheny VK. Drawing the Map of Life: Inside the Human Genome Project. Basic Books. 2010.

[12] Snyder M, Du J, Gerstein M. Personal genome sequencing: current approaches and challenges. Genes Dev. 2010.

[13] Lohr S. The origins of ‘big data’: An etymological detective story, New York Times. 2014.

[14] Bennett CC, Hauser K. Artificial intelligence framework for simulating clinical decision-making: a Markov decision process approach. Artif Intell Med. 2013.

[15] Hampton T. Disease, drug response linked to loss or gain of big DNA chunks in genome. JAMA. 2007.

[16] Bachrach Y, Kosinski M, Graepel T, Kohli P, Stillwell D. Personality and patterns of Facebook usage, WebSci ’12: Proceedings of the 3rd Annual ACM Web Science Conference. 2012.

[17] Bollen J, Mao H, Zeng X-J. Twitter mood predicts the stock market, Journal of Computational Science. 2011.

[18] Kuehn BM. NIH Recruits Centers to Lead Effort to Leverage “Big Data” JAMA. 2013.

[19] Collins FS, Varmus H. A new initiative on precision medicine. N Engl J Med. 2015.

[20] Marx V. Biology: The big challenges of big data. Nature. 2013.

[21] Weber GM, Mandl KD, Kohane IS. Finding the missing link for big biomedical data. JAMA. 2014.

[22] Daughtery SE, Whaba S, Fleurence R. Patient-powered research networks: building capacity for conducting patient-centered clinical outcomes research. JAMA. 2014.

[23] Fleurence RL, Curtis LH, Califf RM, Platt R, Selby JV, Brown JS. Launching PCORnet, a national patient-centered clinical research network. J Am Med Inform Assoc. 2014.

[24] Clancy C, Collins FS. Patient-Centered Outcomes Research Institute: the intersection of science and health care. Sci Transl Med. 2010.

[25] Schneeweiss S. Learning from big health care data. The New England Journal of Medicine. 2014.