IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
IJARSCT
Impact Factor: 6.252
Volume 2, Issue 2, April 2022

Leveraging Block Chain for Ensuring Trust in IoT in Health Care

Yesha Gandhi[1] and Sandip Chauhan[2]
P. G. Student, Department of Information Technology[1]
Faculty, Department of Information Technology[2]
Shantilal Shah Engineering College, Rajkot, Gujarat, India

Abstract: *Internet of Things (IoT) devices has completely new challenges regarding security and privacy. Blockchain technology could be a great to mitigate challenges of data security and privacy relay in the IoT. Crypto currency networks like Bit coin, can prove to be required towards understanding concept of decentralized, security and Leveraging of blockchain for privacy preserving. Differential privacy is a mathematical technique of adding a controlled amount of randomized noise to a dataset to prevent anyone from getting information about individuals in the dataset. The added randomized noise is in controlled manner. Therefore, the resultant dataset is still accurate enough to generate aggregate output while maintaining the privacy of individual participants. As Block chain is a peer-to-peer distributed ledger, it is an optimal way for preventing identity, monitoring, non-repudiation and providing tracking in IoT, so due to these aspects we can explore future research challenges to preserve privacy in blockchain.*

Keywords: Blockchain, differential privacy, E-health records, Utility Trade-off

I. Introduction

The blockchain is a distributed database of records of all transactions. Blockchain Technology Record Transaction in Digital Ledger which is distributed over the Network. There is no Central Server or System which keeps the data of blockchain. Block chain is a peer-to-peer distributed ledger. It could be a great tool to mitigate challenges of security and privacy relay in the IoT. Hence, we are going with one of the most useful methods Differential privacy. It is a mathematical technique of adding a controlled amount of randomized noise to a dataset to prevent anyone from getting information about individuals in the dataset. First of all, private data of patient is uploaded on digital ledger that is one type of database. That data can be available for patients, their doctors and Medical Store (pharmaceutical person). Each of them can edit or view that data. But the third unauthorized person should not view or edit that data so for that we have to prevent the attack performed on data .For preventing attack, there are various methods available but we have chosen Differential Privacy Mechanism.

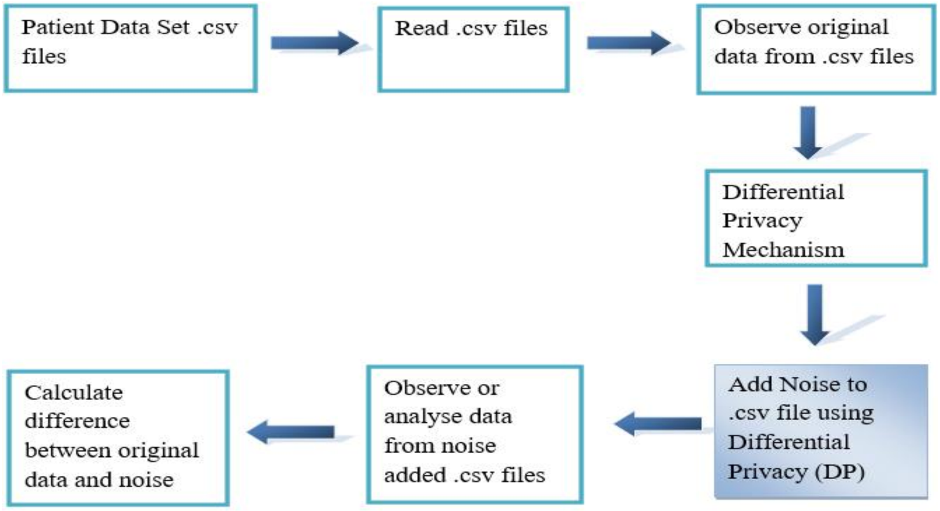
The added randomized noise is controlled. So, the resultant dataset is accurate enough to generate aggregate output while maintaining the privacy of individual participants. Differential privacy can be divided in two types locally or globally. In local differential privacy, noise is added to individual data before it is centralized in a database. In global differential privacy, noise is added to raw data after it is collected from many other individuals.

II. Differential Privacy

2.1 Differential Privacy

In today’s era personal information has become more digitized, it has being more crucial to protect user data. One prevalent technique to achieve this task includes differential privacy. Differential privacy is mathematical definition capable of quantifying the anonymization and security of one’s data within a network, described mathematically. Differential privacy relies on the parameter epsilon to determine the loss in privacy through the addition or removal of specific data. This trade-off between adding “noise” to a dataset to increase its anonymity also decreasing the usability of the actual data, with this trade-off being another method to describe the parameter epsilon (ϵ). Various values of ϵ have been experimented with to determine the proper noise for different applications. By utilizing a differentially private database and providing protection to the user’s identities, this allows of “deniability” as to the inclusion or exclusion of certain patients within a dataset due to the overall results only being affected by a factor of epsilon during each iteration of the differential privacy mechanism.

DOI: 10.48175/IJARSCT-3171


Patient Data Set .csv files
Read .csv files
Observe original data from .csv files
Differential Privacy Mechanism
Add Noise to .csv file using Differential Privacy (DP)
Observe or analyse data from noise added .csv files
Calculate difference between original data and noise

2.2 Principles of Differential Privacy

The basic and fundamental features of differential privacy are as follows,

- It only works for interactive scenarios.
- It can’t provide good results for complex queries.
- When there is a diversity in data, it includes too much noise which ultimately reduce the data utility. DP offers a very neat privacy guarantee and, unlike privacy models in the *k*-anonymity family, does not make assumptions on the intruder's background knowledge.

III. Literature Review

Table 1: Comparison of Literature Survey

Sr No.	Title	Authors	Year Of Published	Advantages	Disadvantages
1	Block chain for Internet of Things: A Survey	Hong-NingDai, Zibin Zheng, Yan Zhang	2019	increases trust, security, transparency	Scalability, Storage
2.	Privacy-preserving solutions for Blockchain: review and challenges	Jorge Bernal Bernabe, Josel. Canova’s, Jose L. Hernadez-Ramos, Rafael Torres Moreno and Antonio Skarmeta	2020	Faster traceability, fast processing	Transaction linkability, crypto-keys management usability, interoperability, or compliance with privacy regulations, such as the GDPR.
3	Differential privacy in blockchain technology: Afuturistic approach	Muneeb Ul Hassan, Mubashir Husain Rehmani Jinjun Chen	2020	Ensure that regardless of whether an individual record is included in the data or not	When there is adiversity in data, it includes too much noise which ultimately reduce the datautility.
4	Differential-Privacy-Based Blockchain Architecture to Secure and Store	Avery W. Huang, Adharsh Kandula, Xiaodi Wang`	2020	Automatically adjusts the accuracy of query results.	Misinterpretation of data, Bio-Surveillance risks

	Electronic Health Records				
5	Normative and Empirical Evaluation of Privacy Utility Trade-off in Healthcare	Syeda Amna Sohai	2021	By adding appropriate amount of noise, we can make our data secure from attacks	If someone adds high noise, query evaluation gives false results so uneven noise reduces utility
6.	Blockchain-Driven Trusted Data Sharing with= Privacy-Protection	Dan Wang, Jindong Zhao, Yingjie	2021	The traceability of data shared across a network	loss of an accounts private keys can lead to complete loss of funds

IV. Methodology

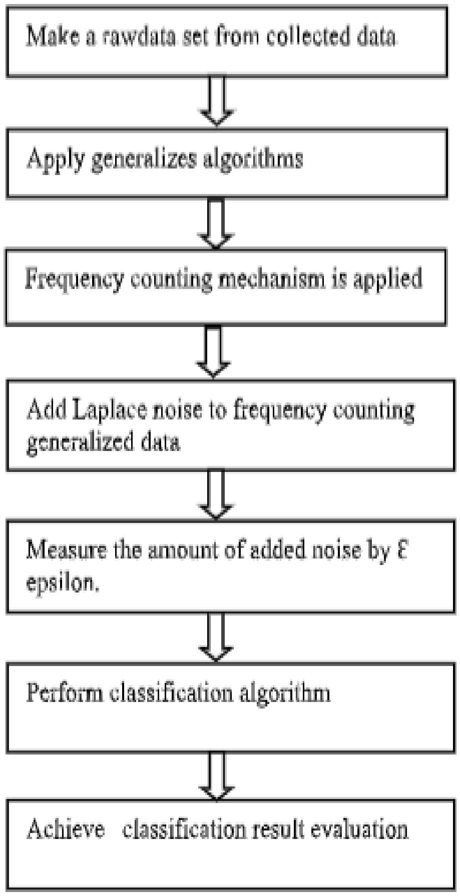

Make a rawdata set from collected data
Apply generalizes algorithms
Frequency counting mechanism is applied
Add Laplace noise to frequency counting generalized data
Measure the amount of added noise by Ɛ epsilon.
Perform classification algorithm
Achieve classification result evaluation

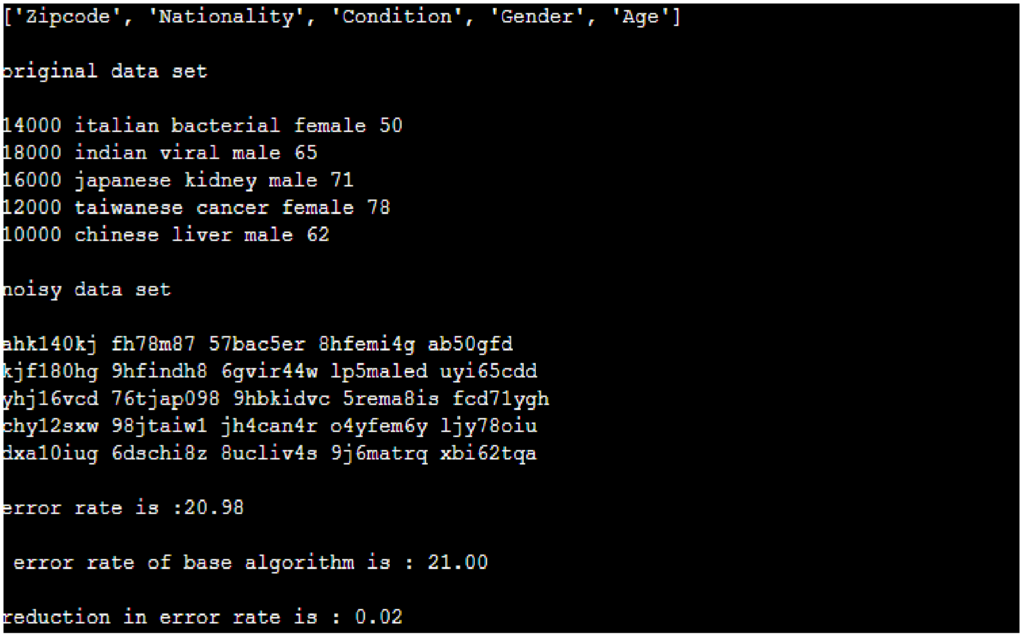
Fig 1. Differential privacy methodology diagram

Our first task is to make a raw dataset from collected data .after making a dataset we have to perform some generalized algorithms on raw data set .Especially, frequency counting mechanism is applied .now it's time to introduce Laplace Mechanism in our algorithm. With the help of Laplace mechanism we are going to add Laplace noise to our generalized data. For measuring the amount of noise that we have added using Laplace Mechanism, we have to figure out Ɛ epsilon factor. So at the last phase we are going to apply Classification algorithms on noise added data and achieve classification result.

V. Result

Proposed algorithms are developed in python language. The result of proposed algorithms is shown in Fig.1. Patients can upload the data set which they want to be secure and preserve. I have taken a dataset which has 5 values namely zip code, Nationality, condition, Gender, Age. I have also shown original dataset without adding any kind of noise. Now using differential privacy mechanism we are adding randomized noise to that dataset so that data set gets secured.

Then I have also shown data set after adding noise. Our base algorithm generated 21% error rate and our proposed algorithm generates 20.98% error rate. So we can observe that we reduce the error rate means our information loss is less than base algorithm.



```
['Zipcode', 'Nationality', 'Condition', 'Gender', 'Age']

original data set

14000 italian bacterial female 50
18000 indian viral male 65
16000 japanese kidney male 71
12000 taiwanese cancer female 78
10000 chinese liver male 62

noisy data set

ahk140kj fh78m87 57bac5er 8hfemi4g ab50gfd
kjf180hg 9hfindh8 6gvir44w lp5maled uyi65cdd
yhj16vcd 76tjap098 9hbkidvc 5rema8is fcd71ygh
chy12sxw 98jtaiw1 jh4can4r o4yfem6y ljy78oiu
dxa10iug 6dschi8z 8ucliv4s 9j6matrq xbi62tqa

error rate is :20.98

 error rate of base algorithm is : 21.00

reduction in error rate is : 0.02
```

Fig. 2 Output of Proposed Methodology

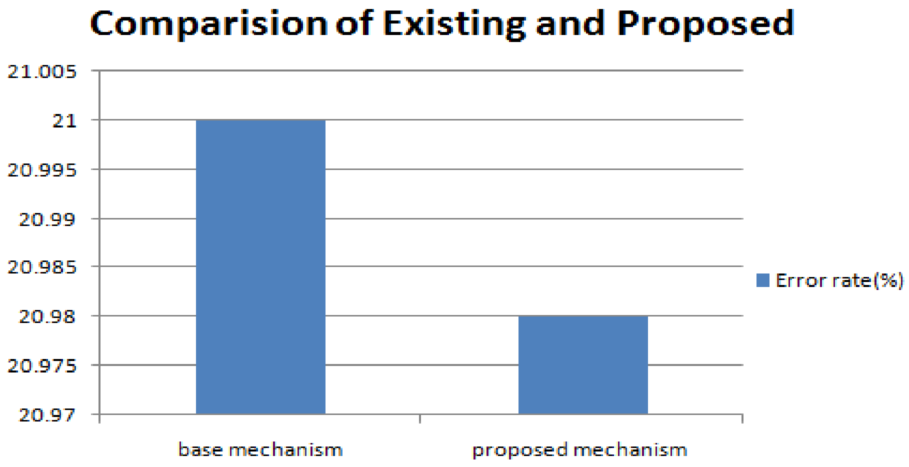


Fig. 3. Comparison between base mechanism and proposed mechanism

VI. Conclusion

DOI: 10.48175/IJARSCT-3171

As Block chain is a peer-to-peer distributed ledger, it is an optimal way for preventing identity, monitoring, non-repudiation and providing tracking in IoT. Existing Algorithm losses information that is shown as 21% error rate and our proposed algorithm shows error rate of 20.98 %, so there is reduction in error rate

VII. Future Work

The future work comprises the quantification of the data value in healthcare. There is possibility to improve Correctness of parameter epsilon (ϵ) so that we can get more accurate result after applying adequate amount of noise. There are certain technologies available for privacy preservation but still further research work can be done in this area.so in future we can work on decreasing complexity with maximum privacy and minimal information loss.

Acknowledgment

It is indeed a great pleasure to express my thanks and gratitude to all those who helped me. No one can achieve or success without the help of friendly guidance and cooperation of so many people involved in the work. I am very thankful to my Guide Prof. Sandip Chauhan the person who makes me to follow the right steps during my research work. I express my deep sense of gratitude to for his guidance, suggestions and expertise at every stage. Apart from that his valuable and expertise, suggestions during documentation of my report indeed help me a lot. I would also like to thank my department and Head of the Department Dr. Milind Shah to give me valuable resources of institute and facilities. My special thanks to respected Dr. Mangal Bhatt, the principal of Shantilal Shah Engineering College, Bhavnagar for providing all the facilities to carry out the research work and for making it successful and Faculty of Atmiya University Ms. Divya R. Solanki for guiding me.

References

[1]. Dai, Hong-Ning, Zibin Zheng, and Yan Zhang. "Blockchain for Internet of Things: A survey." IEEE Internet of Things Journal 6.5 (2019): 8076-8094.

[2]. D. Wang, J. Zhao and Y. Wang, "A Survey on Privacy Protection of Blockchain: The Technology and Application," in IEEE Access, vol. 8, pp. 108766-108781, 2020, doi: 10.1109/ACCESS.2020.2994294.

[3]. Bernabe, Jorge Bernal, et al. "Privacy-preserving solutions for blockchain: Review and challenges." IEEE Access 7 (2019): 164908-164940.

[4]. Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Differential privacy in blockchain technology: A futuristic approach." Journal of Parallel and Distributed Computing 145 (2020): 50-74.

[5]. W, Huang, Avery, Adharsh Kandula, and Xiaodi Wang. "A Differential-Privacy-Based Blockchain Architecture to Secure and Store Electronic Health Records." 2021 The 3rd International Conference on Blockchain Technology. 2021.

[6]. Sohail, Syeda Amna. "Normative and Empirical Evaluation of Privacy Utility Trade-off in Healthcare." Proceedings of the 33rd International Conference on Advanced Information Systems Engineering CAiSE. Vol. 21. 2021.

[7]. Mundhe, Pravin, et al. "Ring signature-based conditional privacy-preserving authentication in VANETs." Wireless Personal Communications 114.1 (2020): 853-881.

[8]. Chase, Melissa, Chaya Ganesh, and Payman Mohassel. "Efficient zero-knowledge proof of algebraic and non-algebraic statements with applications to privacy preserving credentials." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2016.

[9]. Tomaz, Antonio Emerson Barros, et al. "Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain." IEEE Access 8 (2020): 204441-204458.

[10]. Kanna, G. Prabu, and V. Vasudevan. "A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data." Cluster Computing 22.4 (2019): 9561-9569.

[11]. Fotiou, Nikos, et al. "A privacy-preserving statistics marketplace using local differential privacy and blockchain: An application to smart-grid measurements sharing." Blockchain: Research and Applications 2.1 (2021): 100022.

[12]. Liu, Xin, et al. "Blockchain-enabled contextual online learning under local differential privacy for coronary heart disease diagnosis in mobile edge computing." IEEE Journal of Biomedical and Health Informatics 24.8 (2020): 2177-2188.

[13]. https://en.wikipedia.org/wiki/Blind_signature

DOI: 10.48175/IJARSCT-3171