RESEARCHERID
THOMSON REUTERS
[COTII 2019]
ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A DISTRIBUTED COLLABORATIVE MODEL FOR PRESERVING PRIVACY IN CITIZEN HEALTH MONITORING SYSTEM: AN OPTIMAL APPROACH

Umar Khalid Farooqui
Research Scholar, Department of CSE, MUIT, Lucknow, India

ABSTRACT

The Government and administration are always keen about health status of citizens as based on this health data various policy formulation and analytics to be done for the betterment of citizens , however it could not efficiently achieved as various citizens are not willing to share their health related data because of varying privacy requirements. Therefore the administrative agencies have only option to collect data from various Primary Health Centers and third parties whose accuracy is always doubtful.
Crowd sourcing helps scientist to collaborate on large scale health project . Crowd sourcing has been observed as a faster and better alternative to traditional methods for predicting and monitoring infectious diseases. The success of this type of crowd sourcing is depending on the trust on underlying system as the user upload decision is based on the firm commitment to preserve their privacy and assurance of not beingre-identified at later stage.
Here we propose a upload mechanism that could fulfill user's diverse privacy requirements while guaranteeing the quality of health care data simultaneously

Keywords: *Privacy, Cloud ,Health Monitoring.*

I. INTRODUCTION

The Government and administration are always keen about health status of citizens as based on this health data various policy formulation and analytics to be done for the betterment of citizens , however it could not totally achieved as various citizens are not willing to share their health related data because of privacy reasons. Alternatively the administrative agencies have only option to collect data from various PHCs and third parties .The policy makers have to take decision based on the collected data whose accuracy is always challengeable.

The advent of crowd sourced technologies helpsin this regard as number of citizens may upload their health information on to cloud based web application or a centralized server in a reliable and hassle free manner, in addition the Government successfully captured much concerned citizens data as a whole which will further be exploited for various policy matters and research works.

Crowd sourcing helps scientist to collaborate on large scale health project such as ‘pandemics’. Experts also attracted towards crowd sourcing as a faster and better alternative to traditional methods for predicting and monitoring infectious diseases.

However the success of this type of crowd sourcing is depending on the trust on underlying system. The user is always seeking firm commitment to preserve their privacy and win a promise of not being identified /exposed at later stage.)

Crowd sourced healthcare monitoring system utilizes omnipresent smartphone users to upload there health data for investigation and experimentation of various diseases and medicines.

It results in bringing new treatments to faster and also bridges gap between patient and healthcare provider.
In this paper we propose a privacy preserving upload mechanism that could fulfill user's diverse privacy requirements while guaranteeing the quality of health care data.

The quality of health care data depends on the number of uploads by its citizens. The greater no of upload by citizens leads to great quality of collected healthcare data. The decision of uploading by user process is crafted as a mutual objective optimization problem (user anonymity and healthcare data quality) based on an incomplete information game model in which player can independently decide to upload or not to upload healthcare data to balance healthcare data quality and individual privacy requirement.

II. RELATED WORK

For collaborative Healthmonitoring systems, smart phone users generally uploaded their GPS samples in an anonymous way to protect their Medical privacy. The anonymization techniques are not adequate for such a purpose [6–8]. Montjoyeet al. [6] studied a fifteen-month mobility trace data ofone and half million individuals and found that four spatiotemporal points are enough to uniquely identify 95% of them.

Though anonymization can hide obvious identifiers, demographic constraints and spatio-temporal characteristics of the samples from an anonymous mobile allow itself to betraced.Various methods to reduce the spatio-temporal correlation against the tracking attack were proposed [8]. These techniques can be classified as either centralized or distributed. In the centralized approaches [9–11],. An obvious drawback of centralized approaches is their dependence onthe trusted privacy server. Once a server is compromised, the privacy of all associated users is disclosed [12].Distributed approaches [4, 13, 14] do not depend on any centralized server, but allow smartphone users to determine when or where to update samples at their own wills. Asa distributed approach, mix-zone anonymizes user identity by enforcing that a set of users enter, change pseudonyms, and exit a mix-zone in a way such that the mappings between their old and new pseudonyms are not revealed. Palanisamyet al. [13] proposed a mix-zone framework to protect location privacy of mobile users traveling on road networks. Liuet al. [14] aimed to address the problem of optimal multiplemix-zone placement. We claim that mix-zones can hardly support traffic monitoring because users can not upload their locations before exiting a mix-zone. In [4], Hoh et al. proposeda system to specify geographic markers that indicate where vehicles should provide location updates. These markers can be placed to guarantee the maximum tracking uncertainty and to avoid particular privacy sensitive locations. Nevertheless, the markers can hardly meet the diverse privacy requirements of all users. Our approach not only allows users to control their own privacy, but also achieves adual goal of traffic estimation quality and user privacy.
As game theory is suitable for investigating strategic decision-making of multiple players with different objectives, there has been a growing interest in applying game-theoretic approaches to study the issues of mobile network security and privacy [15–18]. Freudiger et al. [16] analyzed the noncooperative behaviors of mobile nodes in a popular location privacy protection mechanism (mix-zone) with a game theoretic model. Yang et al. [17] provided a truthful auction based incentive mechanism for mobile users to join an anonymous set so that k-anonymity can be achieved. Shokri et al.[18] studied the location-privacy of mobile users in location based services (LBSs) by using the framework of Stackel berg Bayesian games. In our approach, we adopt an incomplete information game to analyze the behaviors of smartphone users with mutual objectives (Medical privacy vs. Health Monitoring service quality) in a crowd sourced traffic monitoring system, and propose a privacy-preserving upload mechanism.

III. SYSTEM MODEL

In healthcare monitoring system, each citizen is required to periodically upload his/her health data samples which can be used to estimate the real time health monitoring of the citizens by a server. on the other hand the citizen can get new treatment s to market faster also predicting & monitoring of infectious disease become easier using crowd sourcing.

In reality the accuracy a health monitoring of citizen, i.e. , QoS of Q of the health care service over a period of time, depends on the number of ‘k' of the involved smartphones users who uploaded their health data periodically
Assume a set of smart phone user P = {1, 2-----n } in a group of citizens willing to provide the health samples because they expect to get a better Q Keeping the fact that citizens have different privacy levels
The privacy loss caused by uploading a sample is denoted by 'C’

The accuracy of health care monitoring Q depends on the number 'k 'of involved smartphone users in a group of citizens large k leads to a larger value of Q For the study purpose we categories citizens in to following
a) non adult
b) adult
c) old age
the samples uploaded by non adult are either supervised or not a real sample because of childhood.
Also the adults between 18 to 30 are likely to participate with full zeal where as adults between 31 to 49 are more concerned about their privacy on the other hand old age people are either reluctant or scared towards privacy and security concern.

IV. PROBLEM DESCRIPTION

4.1 health monitoring quality

The accuracy of healthcare monitoring depend on the number of upload users
Let S_i Be the upload strategy of user 'i' with two possible values upload (y) or not (N)
Then,Let Q_i denote the accuracy of health monitoring in a group of citizen 'i' which can be logarithmically represented as

$$Q_i = \log_\alpha(1 + K_i\beta) \quad \text{.....(1)}$$

Where α and β are system parameters and $\log_\alpha (1 + K_i \beta)$ term reflects the Q_i'sdiminishing return on K_i , the numberof upload users.We can obtain value ofα and β from an empirical study on Q by using unconstrained nonlinear minimization over real world data.
The (1) can also be written as

$$Q = log_\alpha(\mathbf{1} + \boldsymbol{\beta} \sum_{i=1}^{n} I\,(S_i, \mathrm{Y}) \quad \text{.....(2).}$$

Where I (x,y)= 1 , if x=y and 0 otherwise.
the objective is to guarantee the upload strategy profile (S_1 ,S_2 -----S_n) of the user such that $Q \geq Q_{min}$
Where $Q_{min}$is the minimum service quality requirement.

4.2 Medical Privacy

Most people have a strong sense of privacy in relation to the exposure of their body to others this is an aspect of personal modesty. Medical privacy help in the practice of maintaining the security and confidentiality of patient records get invoice but the conversational discretion of healthcare providers and the security of medical records.
The advent of electronic medical records (EMR). And patient care management system (PCMS) have raised new concerned about privacy, balanced with effort to reduce duplication of service and medical errors. USA have health insurance portability and accountability act (HIPSA) is disclosure regulation (not a privacy law)

What information is in medical records:-
it may includes following

- Basic demographic data such as address, age, gender, And race
- Full name and account number and sometimes Aadhaar No./patient ID
- Medical history, diagnosis, treatments, diagnostic test result, and prescriptions, along with non medical conditions allergies and drug /alcohol/smoking habits
- Billing and payment information

There is also pharmacy benefit manager (PBMs) which administer drug benefit programs for health plans. PBMs have your entire prescriptions history drug date dosage and who prescribed them, because part of their role is to check your eligibility and get approval for your medication. They also sell DEIDENTIFIED INFORMATION (not covered by HIPPA because personal identify bill information has been removed) to data miners.

The identity of user is determined by tracking incorrectness and identity uncertainty of the user. The adversary's goal is to extract a subset of samples generated by the same person/device ,given a series of sample mixed from multiple users.

The adversary shall be prone to utilize 'Qasi-Identifiers' available with the sample(s) to perform **re-identification** of the user.

The adversary associates a prior upload sample with the next one closest to its prediction, or with the most likely sample. The formulation is described below.

arg max p(x | x_{i-1}) ……(3),

where the conditional probability **p(x | x_{i-1})**is defined asthe probability of next upload sample at location x ,given the prior sample at x_{i-1}**.**

The incorrectness of the tracking attack is definedto be the expected distance between the true locationx_i and its estimate based on $\hat{p}(x|x_{i-1})$, which can be computed

by the following sum:$\Sigma_x \hat{p}(x|x_{i-1})\, I_z(x, x_i)$……..(4)

where$I_z(x, x_i)$equals 0 if and only if $\|x-x_i\|<\varepsilon$,with ε being a small positive real number, and 1 otherwise.

We quantify the uncertainty of the identity inference usingthe entropy of the distribution $\hat{p}(P = ID_i|x)$:

$H = \Sigma i \hat{p}(P = ID_i|x) \log_2 1/(\hat{p}(P = ID_i|x))$……..(5)

The entropy H shown above indicates how hard to pinpointa single outcome ID_i out of P at location x. The higherthe entropy, the higher the adversary's uncertainty aboutan identify.

By combining (4) and (5), we obtain the normalized locationprivacy of user 'i' immediately before it makes a decisionregarding whether to upload or not:

$MP-_i = \frac{1}{2}(H/\log_2 n + \Sigma_{x \in R}\, p(x|x_{i-1})\, I_z(x, x_i)$……...(6)

Notice that uploading samples suffers from privacy loss because the adversary can get more informationabout users' and obtain more accurate inference outcomes.Let ci be the upload cost of user i, 0 < ci < 1, thenthe location privacy level according to user i's strategy canbe computed by

$MP_i(s_i) = \{MP-_i - c_i s_i = Y;$ ……(7)
$\{ MP-_i , s_i = N;$

Typically, the higher the privacy level $MP-_i$, the lower the probability of being traced and identified, the lower the cost c_i.

4.3 Optimization problem

Given the minimum service quality requirement $Q_{min}$and the privacy level $MP_i$of each user in a community .The optimization problem is to find out the upload strategy profile S=(S_1 ,S_2 -----S_n) That maximize the total privacy level $\sum_i MP_i$such that $Q \geq Q_{min}$.

The approach must address following two key issues.

1) User may not know other's privacy level and hence hesitate to upload due to high risk of privacy loos on upload.
2) How to estimate the minimum service quality requirement Q_{min}.

For the first challenge, we introduce an incomplete information game model [20] in which each user is assigned a type θ, whose probability density function $f(\theta)$indicates the distribution of the user's privacy level. In other words, each user is aware of only the privacy level distribution, not the actual privacy level. For the second challenge, we exploit the server's global view (i.e., historical health status of citizens) to estimate the minimum service quality requirement.

V. GAME MODEL

To model the upload decision process of smartphone users we introduced the incomplete information game
In this game each player (citizen) balance their health information privacy (medical privacy) and accuracy of 'health monitoring' to determine whether or not to upload.

Set of player p={1,2,3----n},
Corresponds to the set of smartphone users in a specific group of people.
Each player has two possible moves: upload (y) or not (n).
Bayesian Nash equilibrium (BNE) of user upload game can be obtained by comparing the average utility of 'y' with that of 'n'.

The optimum solution to the strategy of user i is based on health monitoring service quality and the medical privacy level of the user, also the utility of user i is defined as :

$$\mathbf{U_i(S_i(\theta_i), S_{-i}(\theta_{-i}) = w\, Q_i(S_i(\theta_i), S_{-i}(\theta_{-i})) + MP_i\, S_i(\theta_i)} \quad \text{.....(8)}$$

Where $Q_i(S_i,S_{-i})$ is the health care monitoring service quality determined by the moves of user i and its opponent –i ,$MP_i(S_i)$ is the medical privacy of user i.
Also w can be considered as the expectation degree of users to Q.
θ_i is the privacy level immediately before the game.

5.1 Nash Equilibrium

The concept of Bayesian Nash Equilibrium [16] for theincomplete information game is introduced as follows.
: A strategy profile $s*= \{s*_i(\theta_i); s*_{-i}(\theta_{-i})\}$
is a pure-strategy Bayesian Nash equilibrium (BNE) if, foreach player i:

$$\mathbf{s*_i(\theta_i) \in argmax_{si\in\{Y;N\}} \Sigma f(\theta_{-i}) u_i(s_i, s*_{-i}(\theta_{-i})), \forall \theta_{-i}} \quad \text{.....(9)}$$

The BNE in our user upload game can be obtained bycomparing the average utility of Y with that of N, as follows:

$$\mathbf{E[u_i(Y, s_{-i})] = wE[Q(Y, s_{-i}(\theta_{-i}))] + MP_{-i} - ci}$$
$$\mathbf{E[u_i(N, s_{-i})] = wE[Q(N, s_{-i}(\theta_{-i}))] + MP_{-I}} \quad \text{.....(10)}$$

whereY is the NE strategy of user ifor $c_i < w(E[Q(Y, s_{-i}(\theta_{-i}))] - E[Q(N, s_{-i}(\theta_{-i}))])$, and N is the NE strategy of user ifor $c_i \geq w(E[Q(Y, s_{-i}(\theta_{-i}))] - E[Q(N, s_{-i}(\theta_{-i}))])$.

We denote the upload probability of user iby $p_i = \int_{\theta_i}^{1} f(\theta_i) d\theta_i$, where $\theta_i$is the minimum privacy level at whichuser 'i' is willing to upload. Let $P_Y$be a subset of k uploadusers in the given set P; thus the probability thatthe number of upload users is equal to k is $Pr(K = k) = \Pi_{i\in PY} p_i \Pi_{j\in P-PY}(1 - p_j)$. Therefore, the average qualityof Health information estimation is shown as follows:

$$\mathbf{E(Q) = \Sigma^{n}_{k=1} Pr(K = k) \log_\alpha(1 + \beta k)}, \quad \text{.....(11)}$$

and there exists ^k such that $\log_\alpha(1 + \hat{}k\beta) \approx E(Q)$. Hencewe have

$$\mathbf{E[Q(Y, s_{-i}(\theta_{-i}))] - E[Q(N, s_{-i}(\theta_{-i}))] \approx \log_\alpha 1 + \beta(1 + \hat{}k)/(1 + \beta\hat{}k)} \quad \text{.....(12)}$$

From here we can rewrite the upload threshold as :

$w\log_\alpha(1+\beta(1+\hat{}k)) / (1+\beta\hat{}k)$.

VI. THE UPLOAD MECHANISM

Our design goals is to provide users with an appropriate level of privacy preservation and to achieve an overall optimality of the "Health care monitoring system" quality and "Medical Privacy" of the person.

6.1 Upload Algorithm

The proposed privacy preserving medical data collection algorithm is mentioned here, which uses a game of incomplete information and ensure k-anonymity of the upload data, It comprises of three phases.

6.1.1 The 'k' estimation phase :

Firstly the server estimates required number of upload users according to the historical health status of citizen.
Here we present the functional relationship between the asked quality of health monitoring in a population and the historical computation of average number of patients 'n'.

$$Q(n) = (P / (\sigma\sqrt{2\pi})) e^{-(n-\mu)2/2\sigma2} \quad \text{.....(13)}$$

Where P>0 , is a system parameter ,μ and σ are mean and standard deviation and n is the historical estimate of the average patients.
Further $k= (\alpha^{Q(n)} – 1) / \beta$.....(14)

Where 'k' is the required number of upload users we required.

6.1.2 Upload user Selection Phase : (optimizer)

Each user compute w for which Nash Equilibrium can be obtained and then decide to upload or not based on value of 'w'.

If the players(user) knows the upload cost of oponentsi.e, c1 ≤ c2 ≤ c3 ….. cn.Then it is simple to get value of w as :
$W= C_k / (\log_\alpha(1+ \beta (k+1))/(1+ \beta K).$

However user does not know privacy level and privacy cost of others due to incomplete information model,we need to compute the value of C_k.
We assume that $MP_i= \lambda / C_i$, also the privacy level have distribution $f(\theta_i)$,we get
$k/m = \int_0^1 f(\theta i) d\theta i$ .....(15)

where m is the number of smart phone users in a population. The value of w could be given as-

$W = \lambda / (F^{-1} (1- k/m) \log_\alpha (1+ \beta (k+1))/(1+ \beta K))$.....(16)

6.1.3 GenReqalgorithm :

INPUT : request r = < a_1,a_2,……a_i>
OUTPUT : k-minimal generalized request r' = < a_1',a_2',……a_i'>

1) r' ←φ
2) for each a_i **in r do:**
   a) temp ← Max(a_i)
   b) while(true)
      i. k ← Query(temp)
      ii. if (k+1 < k) then
          break;
      iii. a_i' ← temp
      iv. temp ←PrevGen(temp)

v. if (temp=a_i) then
break;
c) if (a_i'= φ) then
i. r' ← φ
ii. break;
3) return r'

6.2 The Privacy preserving upload Model

We devise a privacy preserving distributed upload model which first compute number of required upload at server and then the user is empowered to make decision to upload or not based on the computed value of 'w' , which is further depending on the upload cost and given that the user does not know the privacy level and privacy cost of others ,so we use an incomplete information game model ,and based on NE final computed value of w is obtained. Further the value to be uploaded are generally medical records/ health information of citizens and the user never want to be re-identified from these uploaded record ,thus we use upload model which works on the basis of GenReq algorithm and finally achieve k-anonymity of health records.
Following figure depicts a glimpse of proposed model.

ISSN 2348 – 8034
Impact Factor- 5.070

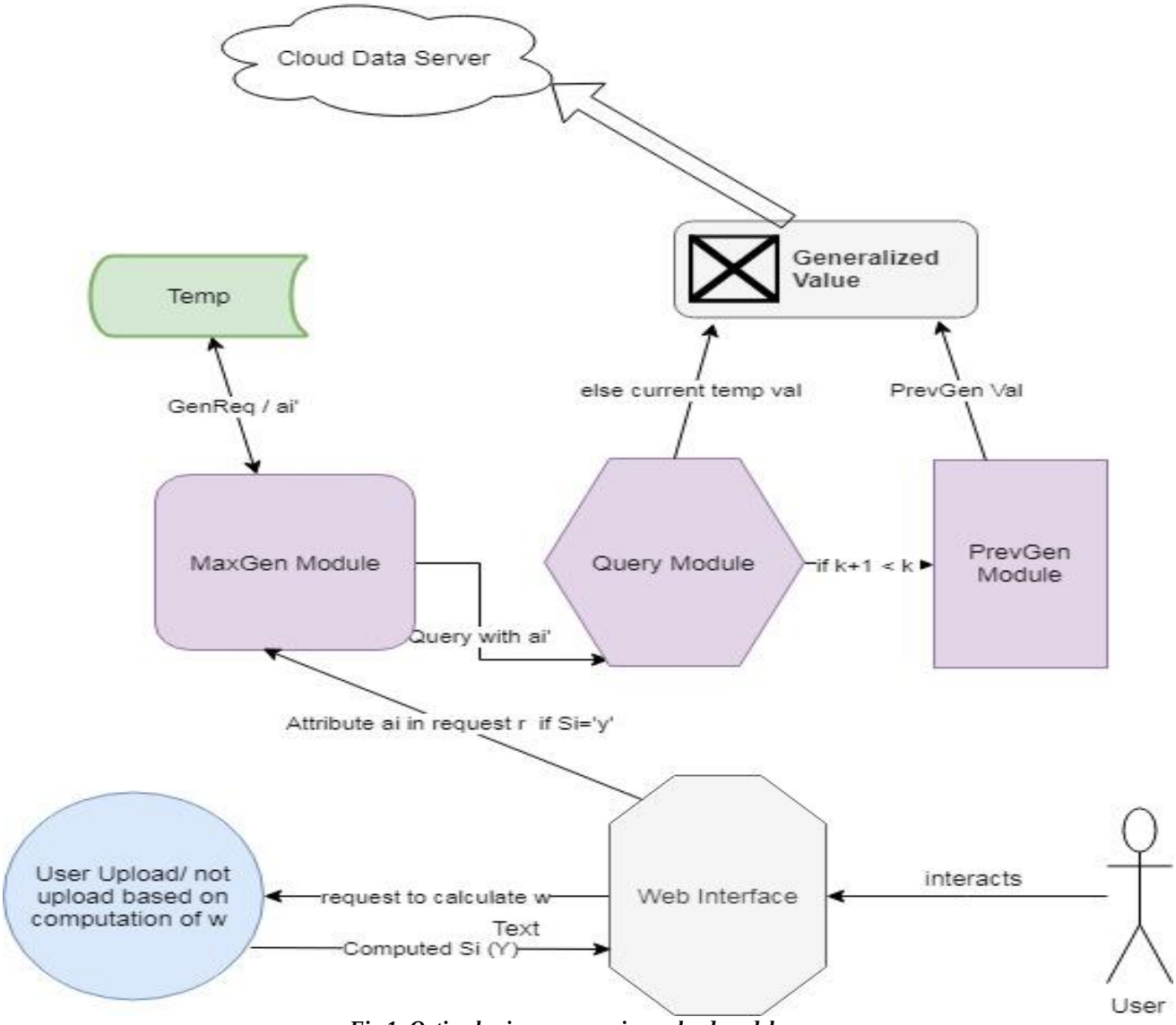

Fig 1: Optimal privacy preserving upload model

The user first interact with the interface and initiate request at this time the request is passed through optimizer and directed to the server while passing Q(n), i.e. the asked quality of health monitoring in terms of average number of patients 'n'in a population ,now the server computes value of k (i.e, required number of upload users) and send it back to the optimizer next the optimizer compute value of w based on the received value of 'k'.finally based on the computed value of w the user is empowered to take decision to upload or not.

As the upload records are health information and are interrelated so there exist a strong requirement of assuring k-anonymity property and for that we use a distributed collaborative model which has no single point of failure.The working of distributed collaborative model is given below.

Firstly the MaxGen node receives a request r with attribute $a_i$from a user i, next it returns maximum generalized value of the supplied attribute and stored it in ***temp***.

The Query Server queries peers of i with this attribute value(a_i) to see how many of the peers of i have the same value in their list.Each peer replies just "yes" or "no" and finally Query Server sums up the total number of positive answers in k. Now if k+1< k , it means that the current value of the attribute does not satisfy the k-anonymity requirement with respect to current time and the previous value would be the best one to use.

The PrevGen Node returns the previous generalized value from the generalization list of attribute. The returned value is the less generalized one that precedes the one passed as an argument, and if k+1< k then this value will be saved as the attribute of the generalized request.

Otherwise the current temp value will be saved as the attribute of the generalized request.
For each attribute in r ,it performs the loop operation and finally form the generalized request r'.

Finally these generalized requests are uploaded to the Heath care monitoring server generally hosted in cloud environment.

VII. CONCLUSION

We propose a privacy preserving upload mechanism to preserve user's medical privacy in a collaborative health monitoring system. The approach is user centric and create an equilibrium between user's medical privacy and healthcare monitoring system .

The quality of underlying Health care monitoring system depends on the number of uploaded samples by number of citizens/users in a population, also the citizen hesitates in uploading due to high concern of privacy leak or risk of re-identification. We address this issue by first calculating required number of upload which depends on number of patients in a population segment. Further the user is assured for required level of privacy by using user upload strategy based on an incomplete information game model which uses benefits of Bayesian-nash equilibrium.
In this system health records are interrelated and sometimes subjective too ,also it has been learnt that the user may be re-identified at later stage by evaluating pair of values. We address the issue of k- anonymity of the uploaded health record by implementing PrevGen Algorithm in our model which results in generalized value saved into cloud database and thus assured k-anonymity of the health records .

REFERENCES

1. *Khalid Farooqui, Umar. (2018). A Comparative Study on Privacy Preserving Schemes based on Encryption Proxy and Cloud Mask. International Journal for Research in Applied Science and Engineering Technology. 6. 401-405. 10.22214/ijraset.2018.3064.*
2. *He, Yunhua& Sun, Limin & Li, Zhi& Li, Hong & Cheng, Xiuzhen. (2014). An optimal privacy-preserving mechanism for crowd sourced traffic monitoring. Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).2014. 10.1145/2634274.2634275.*
3. *Farzana Rahman, Hoque, Sheikh, ProQuPri, Proceedings of the 2011 ACM Symposium on Applied Computing,2011*
4. *Baik Hoh, TochIwuchukwu, Quinn Jacobson, Daniel Work, Alexandre M Bayen, Ryan Herring, J-CHerrera, Marco Gruteser, Murali Annavaram, and JeffBan. Enhancing privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines. Mobile Computing, IEEE Transactions on,11(5):849–864, 2012.*
5. *Yves-Alexandre de Montjoye, C´esarA Hidalgo, Michel Verleysen, and Vincent D Blondel. Unique in the crowd: The privacy bounds of human mobility. Naturesrep., 3, 2013.*
6. *Chris Y.T. Ma, David K.Y. Yau, Nung Kwan Yip, and Nageswara S.V. Rao. Privacy vulnerability of published anonymous mobility traces. In Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking, MobiCom'10.ACM, 2010.*

7. *Laurent Bindschaedler, Murtuza Jadliwala, Igor Bilogrevic, ImadAad, Philip Ginzboorg, Valtteri Niemi, and Jean-Pierre Hubaux. Track me if you can:On the effectiveness of context-based identifier changes in deployed mobile networks. In NDSS. The Internet Society, 2012.*
8. *Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaf Alrabady. Achieving guaranteed anonymity in gpstraces via uncertainty- aware path cloaking. Mobile Computing, IEEE Transactions on, 9(8):1089–1107,2010.*
9. *Mehmet Ercan Nergiz, Maurizio Atzori, Yucel Saygin,and Bar Guc. Towards trajectory anonymization: A generalization- based approach. Trans. Data Privacy,2009.*
10. *Karen P Tang, Pedram Keyani, James Fogarty, and Jason I Hong. Putting people in their place: an anonymous and privacy- sensitive approach to collecting sensed data in location-based applications. In Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 93–102. ACM,2006.*
11. *Elaine Shi, Richard Chow, T h. Hubert Chan, Dawn Song, and Eleanor Rieffel. Privacy-preserving aggregation of time-series data. In In NDSS, 2011.*
12. *Balaji Palanisamy and Ling Liu. Mobimix: Protecting location privacy with mix-zones over road networks. InData Engineering (ICDE), 2011 IEEE 27thInternational Conference on, pages 494–505.IEEE,2011.*
13. *Xinxin Liu, Han Zhao, Miao Pan, HaoYue, XiaolinLi, and Yuguang Fang. Traffic-aware multiple mixzone placement for protecting location privacy. In The31st IEEE International Conference on Computer Communications (INFOCOM 2012), 2012.*
14. *TansuAlpcan and Sonja Buchegger. Security games for vehicular networks. Mobile Computing, IEEE Transactions on, 10(2):280–290, 2011.*
15. *Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C Parkes. Onnon-cooperative location privacy: a game-theoretic analysis. In Proceedings of the 16th ACM conferenceon Computer and communications security, pages324–337. ACM, 2009.*
16. *Dejun Yang, Xi Fang, and Guoliang Xue. Truth fulincentive mechanisms for k-anonymity location privacy. In INFOCOM, IEEE International Conference on Computer Communications, pages3094–3102, 2013.*
17. *Reza Shokri, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-YvesLe Boudec. Protecting location privacy: Optimal strategy against localization attacks. In Proceedings ofthe ACM conference on Computer and Communications Security (CCS), pages 617–627.ACM, 2012.*
18. *Mudhakar Srivatsa and Mike Hicks. Deanonymizing mobility traces: Using social network as aside-channel. In Proceedings of the 2012 ACM conference on Computer and communications security,pages 628–637. ACM, 2012.*
19. *John C. Harsanyi. Games with incomplete informationplayed by "bayesian" players, i-iii. Manage. Sci., 50(12 Supplement):1804–1817, 2004.*
20. *Koh HC, Tan G. Data mining applications in healthcare. Healthcare InfManag2005;19(2):64–72.*
21. *Jentzsch N, Preibusch S, Harasser A. Study on monetising privacy: an economicmodel for pricing personal information. ENISA; 2012.*
22. *Fung BCM, Wang K, Chen R, Yu PS. Privacy-preserving data publishing: a survey of recent developments. ACM ComputSurv 2010;42(4):14:1–14:53.*