JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

PERSONAL PRIVACY PRESERVING DATA PUBLICATION OF COVID-19 PANDEMIC DATA USING EDGE COMPUTING

Pavan Kumar Vadrevu[1], Sri Krishna Adusumalli[2], Vamsi Krishna Mangalapalli[3]

Received: 14 April 2020 Revised and Accepted: 8 August 2020

ABSTRACT: Data processing and publication is playing a pivotal role today with the advanced technology like IoT and edge computing. Today huge amount of data is coming from the devices which are connected with Internet and they generate the data frequently. Today COVID-19 pandemic data is one of the best examples for continuous data; here the entire world is facing the problem with medical emergency. The data generated must be processed and analyzed the same must be published without violating the personal privacy measures. An edge computing device can perform all the computations which can be performed in any environment like data preprocessing, data analysis etc. It is important to process data before storing into the cloud environment and the same is shared with advisories or data publishers like news papers or electronic media, because it may lead to privacy breach. To protect personal privacy, the measures like differential privacy are incorporated in the system which can provide personal privacy guard to the data. Edge computing technologies having good number of capabilities like efficient data processing near source to reduce bandwidth of the internet, enables security of sensitive data on the public cloud infrastructure.

KEYWORDS: Personal Privacy, Edge Computing, Differential Privacy (DP), Data Publication

I. INTRODUCTION

How to overcome and fight against COVID-19 pandemic is only the issue in front of all the countries today, many countries started research for vaccine and medicine for this decease [5]. It takes some time to get out of this dangerous situation for the entire world [5]. All the countries doing lot of testing for the citizens to stop spreading this virus if the patients are identified government is taking them for the isolation and treatment for COVID-19[5]. In INDIA different state governments are taking different measures and different testing procedures to find out the patients infected with this virus [6].There are two different types of testing procedures like RTPCR (Swab Test) and Rapid Test (Blood Test).Among these two testing procedures RTPCR is more accurate but involves lot of manual procedure also it takes 2 to 3 hour of time to give results. Most of the counties adopted RTPCR testing procedure for this COVID-19. The existing mechanism involves risk for the medical people while taking the sample from the infected patient [6].The privacy of the infected individual is violated by publishing the data to the public without performing any personal privacy preservation mechanisms. The motivation testing procedure (RTPCR) and the case study for Personal Privacy violation is discussed in the following section.

1.1 Motivation

If the person has corona virus symptoms then they will visit the hospital and the doctors take the sample from the patient oral and nasal cavity [1]. The citizen should be in the hospital until the further procedure completes. If the test gets negative then the person will be discharged otherwise the patient gets the treatment of corona virus. Today thousands of people are being testing if they have the symptoms of virus across the world some of the people are not going for testing even they have infected with virus due to fear and spreading the virus to others. Existing testing mechanism is working well to identify the virus with the patient but taking much time to produce result and inform to the authorities [4]. Collecting all the data and processing it is a tough task today. The COVID-19 RTPCR testing procedure is shown in the figure 1.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

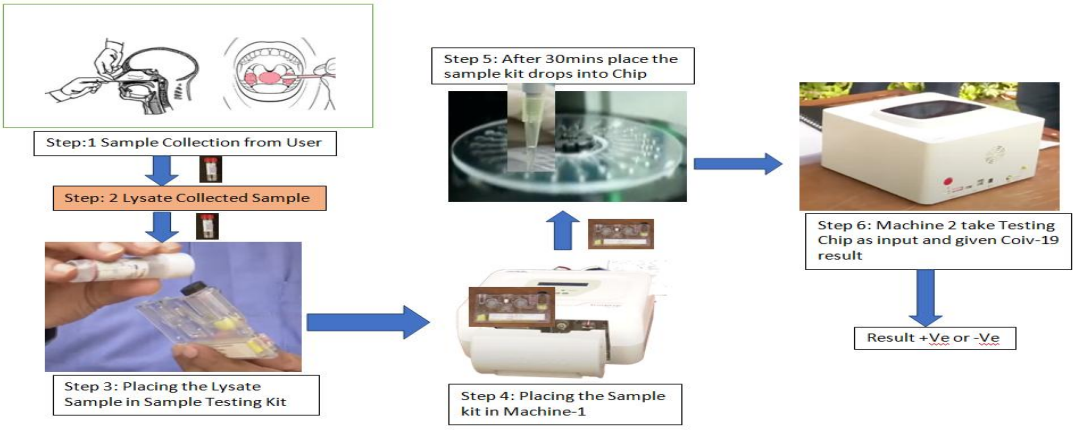


Figure 1 RTPCR testing Architecture

The above mentioned architecture is being followed by many countries to identify the symptoms of COVID-19. This is one of the swab based testing mechanism will give the result by undergoing different processes [1]. This process will take nearly 4 to 6 hours to give the result and is more manual thatis the reason high risk is involved for the medical workers. After completing the test the result is can be given by the authorities to government as well as the individual. If the test result is positive the patient is taken for isolation and can be treated for few days to recover from the decease [1]. The report generation process done by the medical people is manual that means they will take the details of the person like name, age, address etc. if the person is infected with the virus this information along with tested positive given to the government and the same is published in the media this leads to the privacy violation of the individual. Attackers can take the advantage of this published data and that can be given to any insurance agency they take the advantage and they may contact this person after some time to give any insurance policy because high life risk involved at that time the patient feels bad about his leaked information[1]. The example case study for Personal Privacy violation from West Godawari District of Andhrapradesh INDIA is discussed in the following section.

1.2 Case Study

Data publication without protecting personal privacy will definitely leads to personal privacy violation that causes individual feel bad about themselves. Here one example case study taken from the news paper publication during this pandemic period from West Godavari District of Andhrapradesh. If the authorities gives this type of data to media which will be linked throughsome voter list of the location definitely the individual details can be very easily extracted by the third party so that the linking attack leads to a privacy breach. From the above list of data the attacker can easily extract the name and other sensitive details of the individual by

Details of (16) Positive Cases as on 05.04.2020 in West Godavari District

Sl.No	Mandal / Municipality	Village / Area Name	Gender	Age
1	Eluru Municipality	Tangellamudi, Kabadi Gudem	Male	26
2	Eluru Municipality	Tangellamudi, Chakali Veedi	Male	39
3	Eluru Municipality	Tangellamudi Yadav Nager	Male	36
4	Eluru Municipality	Tangellamudi, Near Urdu Boys Govt School	Male	40
5	Bhimadole	Gundugolanu, Kapulapeta	Male	35
6	Eluru Rural	Venkatapuram, Y.S.R.Colony	Male	36
7	Eluru Municipality	Khadar Jhanda, Main Bazar	Male	29
8	Bhimavaram Municipality	Near CPM Office	Male	45
9	Bhimavaram Municipality	Near Veeramma Park	Male	32
10	Penugonda	Maseed Veedi	Male	47
11	Akiveedu Municipality	Kakarlavaari Veedi	Male	48
12	Undi	Balajirao Peta	Male	39
13	Penugonda	Yerrankivaari Veedi	Male	44
14	Eluru Municipality	Tangellamudi, Tilak Nager	Male	27
15	Eluru Municipality	Katheepu Veedi	Male	43
16	Narasapur Municipality	Punja Center	Male	34

Source: News paper article during the month of April 2020

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

doing linking attack through a voter list, which leads to a privacy breach that causes personal privacy violation of the individual. Similarly the government given the data directly during this pandemic situation about the positive cases of COVID-19 on the other day which is very clearly mentioned the sensitive attributes of the individual. In INDIA we do not have perfect privacy policies for the media to publish the data without violating individual privacy. Now a day's government and researchers working on the personal privacy in our country. Here in the below list all the details along with the address of the patient is published after coming out from the treatment from COVID-19 if the insurance agents and companies can take the advantage of this data they may approach the individual can ask for some insurance policy because you have already infected with COVID-19 like that they can talk at that time the individual may feel bad about the situation, because no individual is interested to say I am infected with some kind of decease, that is what here we are calling as personal privacy. If this happens that means the personal privacy of the individual is being violated. From this proposed architecture after completing the testing process of COVID-19 the edge device is going to generate the information about the positive and negative cases without violating the privacy of the individuals. Here in the edge device the mixture of privacy algorithms like K-Anonymity, L-Diversity, Suppression, Tokenization, and Differential Privacy must be incorporated by considering a hybrid algorithm which is going to be identified[8][9].

LIST OF POSITIVES REPORTED ON 25.04.2020 FROM SMC VJA

S.NO.	MSS ID	NAME	AGE	GENDER	ADDRESS	DISTRICT	SAMPLE COLLECTION DATE	SAMPLE RECIEVEING DATE	DATE OF TESTING	RESULT	DATE OF RESULT	SAMPLE CATEGORY	PLACE OF SAMPLE
1	QS-90000449-05	Chinnam Williams	22	M	1-18, ARTHAMURU, UNDI WG	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
2	151710	Shaik Aayisha Begum	18	F	Muslim Street Bheemavaram	WG	17-04-2020		23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
3	151841	Kaamana Durga Rao	40	M	19th Ward, Bhimavaram	WG	17-04-2020		23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
4	QS-90001106-05	Sk Baji	57	M	H/1/34, Pedda Peta Undi - 534 199	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020		
5	182011	P Subba Rao	62	M	16-53, Penugonda	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
6	182860	S Gowri	25	F	Mentevani Thota, Bhimavaram	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
7	182066	Sk Syfulla	56	M	8-9-1, AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
8	182046	Thadi Lakshmi	75	F	10-3-6, Surya Towers, Gowthami Nagar, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
9	182918	Ila Nagamani	39	F	842-11 AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
10	182711	Visanapu Venkata Gowthami	30	F	8-10-11 AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
11	182095	G Satyam	46	M	8-10-19, AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
12	182004	Kodamanchiti Arun Kumar	21	M	8-10-11, AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
13	181957	Sooda Lakshmi Kantham	68	F	8-4-45/2, Opp MPO Office, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
14	182063	Duggina Krishna Chaitanya	20	M	Mentevani Thota, Bhimavaram	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone
15	182044	K Surya Narayana	67	M	8-10-19, AMIS Biriyani Street, Kovvuru	WG	21-04-2020	21-04-2020	23-04-2020	POSITIVE	25-04-2020	General Category	Containment Zone

Source: News paper article during the month of April 2020

Many data scientist working on it to give sufficient information about the active, tested, discharged and deceased patient details. In some of the places the governments publishing the details without violating the privacy of individuals but in some places complete information about the patients including the sensitive attributes like name, address are also publishing, with this definitely leads to the personal privacy violation of the individuals[5]. This scenario was the motivation to start working on the edge computing to protect personal privacy and to process data within the proposed system the data is being sent to the authorities with the required details and the same can be published without violating the personal privacy concerns of the individuals[7][8[9]. This paper is going to propose a testing architecture mechanism by integrating the existing mechanism along with IoT and edge computing so that the involvement of life risk for the medical workers and the details of the patient are safeguarded[7][8][9]. Personal privacy preservation plays a very important role today, for example if the details of the patient (affected with corona virus) are publicly available will leads to privacy violation of the individual [10]. The patient data must be safeguarded when giving it to research or analysis purpose by the Government. Here in this paper a proposal using edge technology after completing the COVID-19 test the information about the infected or non infected individual details sent only to the government and the individual about a positive or negative test report has been sent[7][8][9]. If the person infected with the virus those details are been protected by applying some methodologies like K-Ananonimity, l-Diversity or Differential Privacy

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

[10][11]. The original information is being kept with the government agencies when ever required the ananomized data can be given for research and analysis purpose so that the personal privacy is achieved. Rest of this paper is organized as follows: Section 2 discusses the related work, Section 3 is proposed architecture, Section 4 discusses Differential Privacy (DP) Anonymization Anonymazation Methodology and Section 5 shows the sample experimental results of the proposed work. Finally, conclusion and future scope of the paper is presented in Section 6.

II. RELATED WORK

Andrej Zwitter et al., stated that the Privacy and protection of data are significant principles. They do not fade away all through a crisis. However they have to be weighed next to individual benefits & risks [18].

Zuboff et al., stated that data protection along with privacy are person rights that can be derogated from throughout crisis [18]. They can be provisionally condensed when a public urgent situation call for it. What makes this condition even more complex is the use of data from and by business agencies [18]. Only mentioning the issue of over dominant business power in the form of surveillance entrepreneurship briefly (Zuboff 2019), data ownership is in principle a matter of contract law and in many cases a question of terms of use that customer have to accept by default when intend to use a service [19].

Jean Philippe Walter the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe said that "Several states in Europe and in the world have imposed a state of emergency to fight the COVID-19 pandemic [20]. This situation leads to measures that restrict our human rights and fundamental freedoms, including the right to data protection. These restrictive measures are understandable and justified [20]. However, they should be of a legitimate and exceptional nature and be limited in time. If they involve personal data processing, the basic principles of Convention 108 must be respected, and the rights of data subjects guaranteed" [20].

Shivaji Bhattacharya et al., mentioned that the health authorities, corporate and other stakeholders are taking steps to contain the spread of the virus and measures such as data tracking and mass surveillance could prove to be effective in curbing the spread of COVID-19 [21]. However, keeping in mind that such personal data will be available in the long-term, the Government of India will need to strike the right balance between protection of public interest and maintaining the fundamental right to privacy [21]. Once the COVID-19 enforced lockdown in India eases, corporates in India (regardless of size) will increasingly have to grapple with the processing of SPDI and other personal data to minimize the risk of COVD-19 [21]. To this end, corporates will need to process personal data in compliance with the requirements of the Data Protection Laws while keeping an eye out for potential change in the Indian legal framework on account of the PDP Bill[21].

III. PROPOSED SYSTEM ARCHITECTURE

When the person shows up corona virus symptoms, they can collect their own swab and can keep this into the testing kit by them self with some basic details about the person like name, gender and address[2][3]. This is possible as these testing kits can be much cheaper in future and would be at the hands of every individual. The key idea is to send the results obtained from these kits automatically to the government laboratories for further testing process through a Mobile Application without violating the personal privacy of an individual[2][3]. Also, even the result after this process can be informed back to the individual as well as government by securing the data in the cloud and can be given to the media people using some anonymization techniques so that the personal privacy is being protected[11][12] the proposed architecture as follows.COVD-19 Real Time Reverse Transcription Polymerase Chain Reaction or RTPCR test is prescribed to detect SARS-CoV-2(severe acute respiratory syndrome corona virus 2) or corona virus in respiratory tract through a nasal pharyngeal swab collected from a patient. It detects the virus even if the viral load is less [22].

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

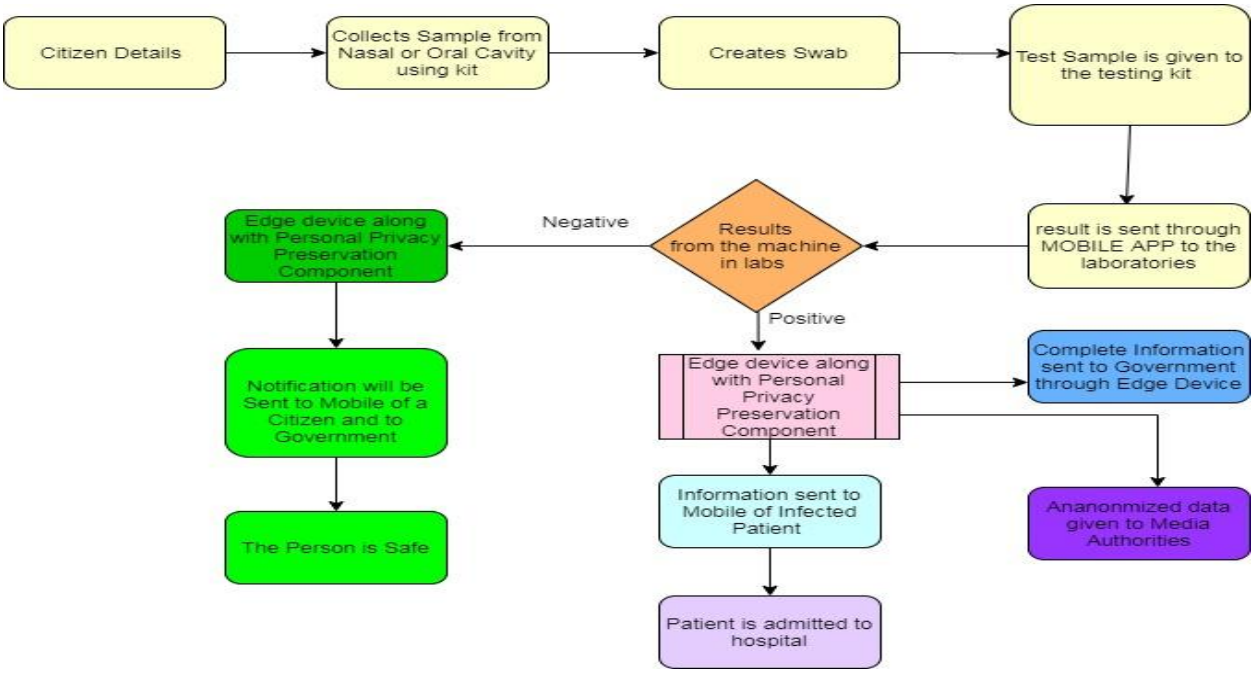


Figure 2 System Architecture

This at home swabbing leads to low spread of infection as the individual need not go to hospitals (in this process this infected individual can infect many others on his way and also can be infected by any other infected one)[1]. This can also reduce the waiting time and can improve testing time. This automation reduces number as well as workload of health care workers [7][8].

Food and Drug Administrative department of US said it believed that, for those people who are exhibiting corona virus symptoms, nostrils swabs "that access just the front of the nose rather than the depth of the nasal cavity" could be used for testing[1]. That would allow people to collect their own samples for testing.

Advantages of Proposed System:

1. These testing kits needs fewer health care workers and are likely to reduce the man power.
2. This also helps to the norms of social distancing strictly.
3. The results of this antibody can be made available within an hour which is a very rapid and the details of the patient kept securely so that personal privacy can be protected.
4. It is portable and can be mounted and transported to anywhere.

From the above proposed architecture the collected sample is sent for different stages of testing the edge device do the entire processing of data and send data to multiple sections. The processed data can be maintained along with some filters by the device. Based on the result the details can be sent to the individual either positive or negative of the test to the mobile device of the individual [7][8][9]. The entire information can be sent to the government authorities for analysis purpose and that cannot be revealed to public. The ananomized data is going to be available for the public along with personal privacy preservation. The information which is going to be sent to the cloud for storage and publication purpose maintained with some key privacy policies maintained under the edge device. The data processing is done by the personal privacy preservation component of the edge device using anonymization techniques, so that the data from the cloud can be given for any analysis or publication purpose[16][17]. Even if the data is published in different media the individual details like name address are not going to be revealed from which we can protect the personal privacy of the individual [7][8][9]. Personal Privacy Preservation achieved using the concept of Differential Privacy (DP) guard mechanism the corresponding ananomization algorithm is explained in the next section.

IV. DIFFERENTIAL PRIVACY AND ANONYMIZATION METHODOLOGY

The main principle of Differential Privacy (DP) involve creation of a data element is not harmed by their access or contribution in a database (DB), while improving utility and data accuracy for the queries [26]. Differential Privacy (DP) [23], projected by DWork, it is accepted hypothesis to offer personal privacy in data publication. The general method to attain differential privacy (DP) is to generate the data with noise [24]. The existing mechanism is for the onetime released data but, here the data generated is continuous in the case of COVID-19 pandemic. Every testing centre is generating data continuously from the testing process. In [25], Wang et al. projected a system achieving w-event privacy. But, their system has limits. Their results on data utility only depend on the data dynamics and ignore the health condition of the user. This paper proposes a real time data

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

publication along with µ-differential privacy (DP) to solve the problem. This proposed scheme provides new personal privacy level for the continuous data streams with adaptive sampling.
A method which satisfies Differential Privacy (DP) must guarantee that the query results remains around the similar if a solitary record is added or removed.

Definition 1 (Differential Privacy [23]): A randomized method M gives µ-differential privacy if for all data sets D and D´ incompatible on at least one, and all O ⊆ range(M),

$$PR [M (D) \in O] \leq \exp (\mu) * PR [m (D´) \in O]$$

µ is the privacy plan. A smaller µ means more noise and strong privacy level. Laplace mechanism is the most common one to guarantee µ-Differential Privacy (DP).

Figure 3 Personal Privacy Preserving Data Publication (PPPDP) Architecture

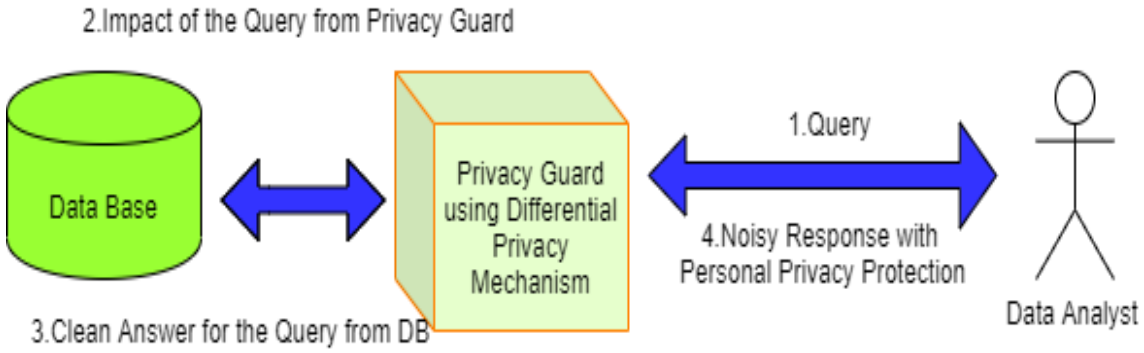


Table.1 Sample Data

MSS ID	NAME	AGE	GENDER	ADDRESS	DISTRICT	SAMPLE COLLECTION DATE	SAMPLE RECEIVED DATE	DATE OF TESTING	RESULT
QS-90000449-05	Chinnam Willams	22	M	1-18,ARTHAMURU	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
151710	SHAIK AAYISHA BEGUM	22	F	MUSLIM STREET, BHIMAVARAM	WG	17-04-2020		23-04-2020	POSITIVE
151841	KAMANA DURGA RAO	40	M	19TH WARD,BHIMAVARAM	WG	17-04-2020		23-04-2020	POSITIVE
168231	SOMA VEERAJU	61	M	WARF ROAD,NARSAPURAM	WG	17-04-2020	18-04-2020	23-04-2020	POSITIVE
171223	S GOWRI	28	F	MENTEVARI STREET,BHIMAVARAM	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
165321	ILLA NAGA MANI	36	F	KOVVURU	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
181234	SODA LAKSHMIKANTH	66	M	MARIYA STREET,KOVVURU	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
152487	G SATYAM	48	M	MIMM BIRYANI STREET, KOVVURU	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
182312	KODAMANCHI ARUN	36	M	KOVVURU	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE
191342	PILLI SUBBARAO	66	M	RAYUDU STREET,NARSAPURAM	WG	17-04-2020	17-04-2020	23-04-2020	POSITIVE

Table.1 considers the raw details of the patients along with the MSS ID (Used for just illustration purpose) each row represents the information about the infected patient. The attributes AGE, GENDER, ADDRESS respectively. Suppose the authorities want to release the details of the Table.1 for the purpose of classification or analysis on these attributes it can be considers as a pair of values like (x to y) without specifying the personal details of the infected patient can be called as a Contingency table represented in the Table.2.

Table.2 Contingency table

DISTRICT	AGE	COUNT
West Godavari	(20-30)	3
West Godavari	(31-40)	3
West Godavari	(41-50)	1
West Godavari	(51-60)	0
West Godavari	(61-70)	3

The preparation of the contingency table is easy to disclose the data; it cannot be affected or extracted with few types of linking attacks, but from the past research if the authorities have partial or full information about the set valued data published then based on the knowledge of attacker they may perform linking attacks to extract more information that means this contingency table also some how vulnerable [27]. This type of personal privacy preservation mechanism also fails in some cases. To prevent this type of problems a partition based personal privacy preserving model is proposed using the concept of Differential Privacy (DP) which is incorporated in

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

the Edge Device to publish or to provide data. The differential privacy methods ensure the chance of released data is approximately uniform probable or of nearly the same for the input data and guarantee the released data insensible to individual data [27]. Thus personal privacy is not in risk because of addition of noise in the disclose data. This proposed methodology is not optimal but it can be considered as a suboptimal solution for the existing personal privacy preservation problem. The anatomization process performs three key steps; first it selects the attribute from the list, second determines the suppression or generalization of the taken attribute, and third publishes the anonymized attribute after adding the noise.

Step 1:

The exponential mechanism is used for selecting the attribute from the list. The entire data from the list is grouped based on the similarity of the attributes, then publishes the noisy count of group. D work et al. proposes the Laplace mechanism [28]. The mechanisms take a data list D, a function F, and the parameter λ that determine the degree of noise as input. It first computes the true output F (D), and then perturbs the output by adding noise [28].

Step 2:

Once the attribute is determined suppression is used to split the taken group of attribute. For numerical values the suppression value is not chosen from the attribute value that is presented in the list D because the probability of selecting the suppression value from a different list D´ not having this value is 0. The probability expression is given as

$$e^{\left(\frac{\mu'}{2\Delta}\right)}\mu(D, Vn)$$

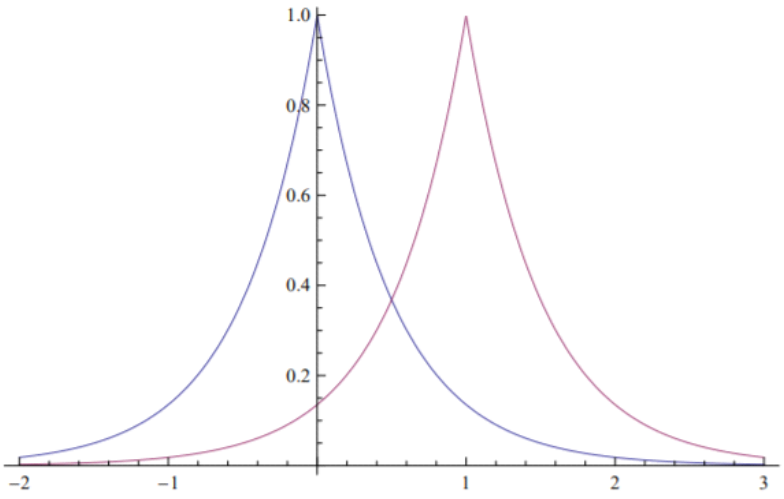
Where D is the data list, μ is privacy budget, Suppression value Vn.

Step 3:

Publishing the anonymized attributes by adding noise with the exact count of attribute group not satisfy differential privacy for a different data list, the count may or may not change. This change can be simply equalized by adding noise to the count of each attribute group according to Laplace mechanism [28].

V. SAMPLE EXPERIMENTAL RESULTS

The experiment is done on a sample data set created for this paper (refer Table 1) available from news paper article published during this pandemic period and the Adult data set available. This experiment given sub optimal solution for the personal privacy preservation problem. The comparison study along with results can be published with the subsequent article. To get μ-differential privacy by adding the noise to the published data computing the sensitivity function F, let us assume that F returns 0.5 if the individual attribute is not in the list, the L-1 sensitivity of F is 0.5 so, to attain differential privacy for μ = 1, we must add a Laplace distribution L (0, 0.5) to the true value of the query output [29]. The sample output of response distribution with addition of noise shown in below 5.1



5.1 Response distributions with noise addition

Let us assume the data analyst is interested in a 0 or 1 output, the value below 0.5 is considered as 0, and the value above 0.5 as 1.

The distribution for the response obtained

$$D = \sum_{k=1}^{n} (F(L(0,1)) \leq 0.5$$

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

VI. CONCLUSION AND FUTURE SCOPE

The mentioned architecture using edge computing technology gives results since the human involvement in the testing procedure is less and the results produced can be directly sent to the individual as well as the government authorities without violating the personal privacy considerations the data can be stored into the cloud for further analysis and research. If the entire process is automated using robotic and IoT technologies can give efficiency and accurate results. We are working on the algorithm for getting better result the work is going to be published in the subsequent papers along with the actual result data.

ACKNOWLEDGEMENTS:

I thank the IT Department and Management of Shri Vishnu Engineering College for Women (A), Bhimavaram for providing all the necessary resources to carry out this work.

AUTHOR AFFILIATIONS:

1. **Pavan Kumar Vadrevu**, Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Paralakhemundi, Orissa (e-mail: vadrevu.pavan@gmail.com)
2. **Sri Krishna Adusumalli**, Associate Professor, Department of Information Technology, Shri Vishnu Engineering College for Women, Bhimavaram , Andhra Pradesh (e-mail : srikrishna@svecw.edu.in)
3. **Vamsi Krishna Mangalapalli**, Professor, Department of CSE, Chaitanya Institute of Science and Technology, Kakinada. (e-mail: vamsimangalam@gmail.com)

VII. REFERENCES

[1] https://www.nytimes.com/2020/03/23/technology/coronavirus-home-testing-swab-kits.html
[2] https://qz.com/1822596/all-the-coronavirus-test-materials-in-short-supply-in-the-us/
[3] https://www.aljazeera.com/news/2020/03/coronavirus-testing-methods-200330142718434.html
[4] https://www.timesnownews.com/health/article/list-of-path-labs-for-coronavirus-testing-in-india-how-and-where-to-get-tested-for-covid/565294
[5] https://azure.microsoft.com/en-us/services/open-datasets/catalog/covid-19-open-research/
[6] https://news.microsoft.com/2020/03/20/adaptive-biotechnologies-and-microsoft-expand-partnership-to-decode-covid-19-immune-response-and-provide-open-data-access/
[7] https://www.cbinsights.com/research/what-is-edge-computing/
[8] https://medium.com/@miccowang/what-is-edge-computing-f997c0ab39fc
[9] https://www.iiconsortium.org/pdf/Introduction_to_Edge_Computing_in_IIoT_2018-06-18.pdf
[10] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[11] Checking Anonymity Levels for Anonymized Data, V. Valli Kumari, N. Sandeep Varma, A. Sri Krishna, K. V. Ramana, K. V. S. V. N. Raju, 7th International Conference, ICDCIT 2011, Bhubaneshwar, India, February 9-12, 2011. Proceedings
[12] A Survey on Personal Privacy Preserving Data Publication in IoT, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8, Issue-6C2, April 2019
[13] https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/
[14] https://blogs.microsoft.com/blog/2020/03/20/delivering-information-and-eliminating-bottlenecks-with-cdcs-covid-19-assessment-bot/
[15] https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/
[16] Privacy- Preserving Data Publishing By Bee- Chung Chen, Daniel Kifer, Kristen LeFevre and Ashwin Machanavajjhala Vol.2, Nos 1-2(2009) 1-67 DOI: 10.1561/1900000008.
[17] The Quest for Privacy in the Internet of Things, PawaniPorambage and Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Athanasios V. Vasilakos, IEEE CLOUD COMPUTING PUBLISHED BY THE IEEE COMPUTERSOCIETY 2016.
[18] https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-020-00072-6
[19] Zuboff, Shoshana (2019) Surveillance capitalism and the challenge of collective action. 28 New Labor Forum 10
[20] https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter
[21] https://www.mondaq.com/india/data-protection/928998/covid-19-implications-on-the-data-protection-framework-in-india
[22] https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/covid-19-rt-pcr-one-test-many-guidelines/what-is-rt-pcr/slideshow/76355749.cms
[23] C. Dwork, “Differential Privacy,” in Proc. of ICALP, 2006, pp. 1–12.
[24] “Differential privacy: A survey of results,” in Proc. of TACM, 2008, pp. 1–19.

ISSN- 2394-5125 VOL 7, ISSUE 19, 2020

[25] Q. Wang, Y. Zhang, X. Lu, and Z. Wang, "RescueDP: Real-time spatiotemporal crowd-sourced data publishing with differential privacy," in Proc. of IEEE INFOCOM, 2016, pp. 1–9.
[26] https://demystifymachinelearning.wordpress.com/2018/11/20/intro-to-differential-privacy/
[27] Privacy-preserving heterogeneous health data sharing Noman Mohammed,Xiaoqian Jiang,Rui Chen,Benjamin C M Fung,Lucila Ohno-Machado, : Mohammed N, Jiang X, Chen R, et al. J Am Med Inform Assoc 2013;20:462–469.
[28] Dwork C, McSherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. Theory of Cryptography Conference (TCC), 2006:265-84.
[29] Improving data utility in differential privacy and k-anonymity arXiv:1307.0966v1 [cs.CR] 3 Jul 2013.