CLOUD- SERVER BASED DATA PRIVACY USING CENTRALIZED AND FEDERATED LEARNING METHODS FOR EHR FRAMEWORK TO SECURE PATIENT DATA

Ms. Cina Mathew[*1] **& Dr. P. Asha**[2]
[1]Research Scholar, School of Computing
[1,2]Sathyabama Institute of Science & Technology, Chennai, India

Abstract:
The effect of insider attack on the e- Healthcare system can lead to false examination of patient health records which have led to unaccountability of data usage and high financial cost as a result of data breaches in the e-healthcare without a highly efficient detection approach. A number of health centers have been faced with legal and reputational consequences as a result. This therefore requires the proposition of an efficient technique that can make this problem addressed most especially eHealth systems on the cloud environment as operations are currently operating with cloud services. Until such approaches are proposed, health records could be attacked and peradventure lead to poor treatment of patients due to misinformation and hence causing the death of individuals. This need serves as a key motivation for this research. In this, we proposed a new framework for detecting insider attacks in Cloud-based Healthcare system using watermarking extraction and logging detection technique. The approach gave an output of the number of activities performed by users with the permission update of legal and illegal intrusion into the system using an audit trail. The proposed approach executed with higher level of precision, recall and accuracy which makes it performs the excellent results.

Keywords: EHR; Trusted cloud server; Deep learning; Patient's health care; Centralized and decentralized method; federated learning; Data privacy.
DOI: 10.24297/j.cims.2023.6.20

1. Introduction

Monitoring the health of the user using cloud- based mobile monitoring system is applied for prevailing the communications through mobile and technologies of cloud computing for providing the feedback of decision support for improving the quality of services in health care domain with low cost. It plays also a risky part about preventing the privacy of the user and monitoring the service providers which adopt the health care technologies. The decryption techniques and unique proposed model named private key proxy for encryption are implemented to shift the complexity of registered parties without compromising the user

privacy. The security and performance of proposed model executed with effectiveness of maintaining the PHR of patient centric model about health information of the patient which is stored and maintained in the third-party database such as cloud storage service providers. There are wide privacy concerns maintaining the PHR to prevent from the third-party services and unauthorized parties.

Finally, our security and performance analysis demonstrate the effectiveness of our proposed design. Personal health record (PHR) is an emerging patient- centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third-party servers and from the unauthorized parties.

Ensure the patient details are preserved and control over the access by their own PHR's which is promising method to encrypt the PHR before storing in the databases of outsource. There are some technical issues like privacy exposure, scalability in maintaining the key management, access data flexibly and revocation user efficient which is more challenging toward cryptography model to enforce the data access control.

Deep neural network is the broad area to shown the unprecedented generalization for different tasks using image recognition for generating the realistic data. The model has led to different applications and services which uses deep learning algorithms on user data for including the speech about the users, images, medical data about user and local data points.

The proposed model has trained for better execution to reach the highest preserved data access control of patient health records. The attribute-based encryption system is an advanced model for encrypting each user data from the PHR file. By securing the data the PHR system developed into multiple security enhanced system for protection of data by reducing the unauthorized access by key generating technique for managing the complexity of owners and users. The preservation of privacy about the data is guaranteed simultaneously by different authority ABE. The dynamic modification of access the data is proposed with different attributes and break glass access under emergency situations with analytical experimental results by enhancing the security, scalability and efficiency of proposed model.

Health care System provides the benefits of streamlined operations, enhanced administration & control, superior patient care, strict cost control and improved profitability. It is powerful, flexible, and easy to use and is designed and developed to deliver real conceivable benefits to hospitals. More importantly it is backed by reliable and dependable support.

Health care System is custom built to meet the specific requirement of the mid and large size hospitals across the globe. All the required modules and features have been particularly built to just fit in to your requirement. This package has been widely accepted by the clients in India

and overseas. Not stopping only to this but they are highly satisfied and appreciating. Entire application is web based and built on 3 tier architecture using the latest technologies. The sound database of the application makes it more users friendly and expandable.

Cloud computing is technology for enabling the convenient, on-demand network access to a share the pool of configurable computing which rapidly released with minimal service provider interaction. Clouds are currently used mainly in commercial settings and focus on on-demand provision of IT infrastructure. Cloud computing can play a significant role in a variety of areas including innovations, virtual worlds, e-business, social networks, or search engines. But currently, it is still in its early stages, with consistent experimentation to come. Without common programming model the cloud computing technology is implemented for developing a common programming models and interfaces, adequate service applications. Avoiding the issues of cloud computing which offered a chance to force the user to protect the data and developers are take an effect in cloudify their applications which was not port them and users use that hand for commercial provider applications.

The proposed research is about to present the framework to design the estimation value and determine the benefits of cloud computing as infrastructure such as self-owned and handled hardware kit. The model is motivated by rising the cloud computing-based service providers for business to use hardware resources which is existing in the operation. The model has no guide to state that the cloud service will do not make sense to do with our work which we want to give outline in technical aspects for valuation approach with cloud computing are considered.

The existing framework that has been employed utilizes either encryption only or watermarking and encryption Approaches. The encryption only approach ensured security and privacy of medical records. This approach combines a list of authorized users which is used for reading and encrypting the records. The data can be encrypted for protecting and decrypted by an authorized user who uses a key. The authorized user can access these data which have been sent to the cloud environment the location of the health center that data is sent. The medium was secured using encryption but malicious insiders could pose an attack on the data by modifying it without being detected. The watermarking and encryption approach was able to detect that a modification have been done by a malicious insider but the insider who performed the action was not detected.

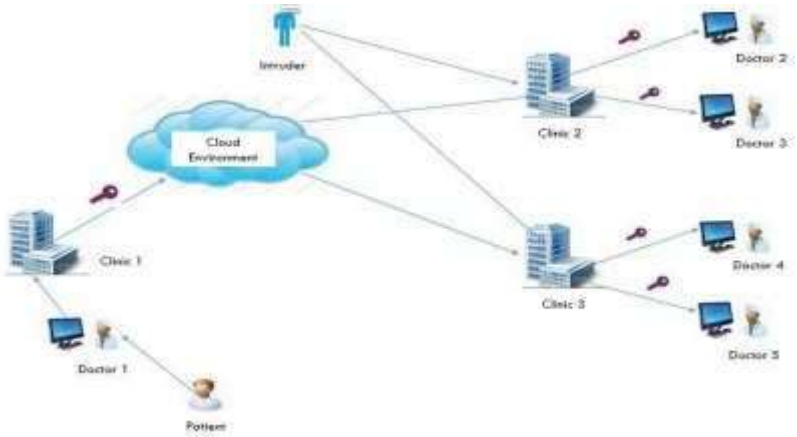

Fig. 1. Cloud connection with private network for data monitoring

2. Literature Survey

Robert H. Deng and Jian: ABE is verifiable outsourced decryption has discussed Attribute-based encryption (ABE) is a public-key base done- to-many encryptions that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied by that user's attributes or access policy into a simple cipher text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. Security of attribute based encryption which helps to encrypt the data which does not guarantee for correctness of transformation of the data using cloud.

Blaze and Strauss, proposed an application called atomic proxy re-encryption", in which a semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. We predict that fast and secure re- encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Ivan and Dodis, they present new re-encryption schemes that realize a stronger notion of security and we demonstrate the usefulness of proxy re- encryption as a method of adding access control to the SFS read-only file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

Susan, et.al., Attribute Based Encryption", has discussed Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes. For example, a user can create a cipher text that can be decrypted only by other users with attributes satisfying. Given its expressiveness, ABE is currently being

considered for many clouds storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the cipher text and the time required to decrypt it grows with the complexity of the access formula. In this work, we propose a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE cipher texts are stored in the cloud. It shows how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE cipher text satisfied by that user's attributes into a El Gamal-style cipher text, without the cloud being able to read any part of the user's messages.

Koteswaramma and S. Lakshmi, has discussed about Mobile health system in which A mobile healthcare system is a network includes a collection of number of components that includes patients and their health-care providers. In this system it is important that the patient to remain connected at all times even if one of the communication components fails. The design of the MediNet system and shows how it faultlessly handles connectivity issues between patients and their mobile phones, between the healthcare meters and mobile phones, and between mobile phones and web server components. The overall goal behind our design strategies is to continue providing a high level of service to the patient in the face of communication problems leading to improved acceptability and trust of the system by patients.

Justin Brickell Donald, et.al., privacy preserving system has discussed present an efficient protocol for privacy-preserving evaluation of diagnostic programs, represented as binary decision trees or branching programs. The protocol applies a branching diagnostic program with classification labels in the leaves to the user's attribute vector. The user learns only the label assigned by the program to his vector; the diagnostic program itself remains secret. The program's owner does not learn anything. Our construction is significantly more efficient than those obtained by direct application of generic secure multi-party computation techniques.

Randal burns, et.al., introduced a model which allows a client that stored a data in untrusted server to verify that the original data without retrieving. The proposed model generates the probabilistic proof of possession by random sets of blocks from the server, number of metadata are verified with the proof. The challenging of protocol transmits a small amount of data, which minimizes network data checking supports large data set in widely- communication. Thus, the PDP model for remote distributed storage systems. It gives two solutions, even provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low, as opposed to linear in the size of the data.

3. Methodology

We hereby propose a framework that has the essential features for detecting any alteration by an insider. The following assumptions hereby exist in our proposed model:

Trusted Cloud and Trusted Third Party are assumed security entities believed to be granted trust by all the Involving health organizations.

i. The secure transmission of keys is not put into consideration based on key exchange policies with the Assumption that every key has been catered for by the prior model and transmitted securely.
ii. A biometric authentication approach is used to access the record R by any doctor in Clinic2 and Clinic3.
iii. We will be using a medical image as the medical record of patient.

3.1. E- Health Record (EHR) Access structure:

The proposed access structure categorizes the users of the EHR into different domains based on their functionalities. There are many different users in the healthcare domain, such as primary care providers, nurses, specialists, pharmacists, medical doctors, and doctors of osteopathic medicine, who focus on family practice, internal medicine, or pediatrics. Each user holds some attributes defined in attribute set. Only those users whose attributes satisfy the access structure defined in the ciphertext are able to decrypt the patient's record successfully. The main advantages of using the proposed access structure are achieving lightweight key management when the number of users is large and mitigating and reducing the workload of the GA responsibility to encrypt the EHR, generate decryption keys, and distribute them to the authorized users.

3.2. Federated Learning method:

Federated learning is also called as collaborative learning method in a machine learning technique which helps to train the algorithms among multiple decentralized servers which holds local data records and it stands to follow the centralized machine learning techniques with all local datasets which are identically distributed. It will enable the multiple bridges to build the robust ML models without sharing or leaking the sensitive data, and it address the critical issues like data privacy, security, and so on. The federated learning has three types as follows,

1. Centralized federated learning
2. Decentralized federated learning
3. Heterogeneous federated learning

3.2.1. Centralized federated learning method:

The central server used to build using different algorithms and coordinate all the active nodes during learning process and the central server is responsible for node selection at initial stage to train the data. All the selected nodes are responsible to send regular updates to single entity.

3.2.2. Decentralized federated learning method:

The nodes are coordinate themselves to obtain the global model to prevent the point failures while exchanging the data between interconnected nodes with the help of central server. But the network topology may affect the performances of learning process at any time.

3.3. Knowledge to priority:

Supervised vs unsupervised learning knowledge as a knowledge method to find the meaningful mapping between models and the data point. Every learning method has a dataset which will overlap the target datasets and it can be train the model in supervised learning method and it leads to attack the training dataset. The mean square error will be reduced in a supervised learning model for predicting the proper datasets in training set.

$$\Sigma_{\boldsymbol{d}\in\boldsymbol{D}'\cap\boldsymbol{D}}(\boldsymbol{h}(\boldsymbol{d})-\mathbf{1})\mathbf{2}+\Sigma_{\boldsymbol{d}\in\boldsymbol{D}'\setminus(\boldsymbol{h}(\boldsymbol{d}))}\mathbf{2} \quad \text{.....(1)}$$

The attack on data has an output for supervised training data is the probability of knowledge testing with datasets. The following equations shows that the probability function of supervised learning sets,

$$H(d) = Pr\ (d\epsilon\ D; f) \quad (2)$$

Also, there is an alternative way for supervised learning method is unsupervised learning method which will be an attack model for target data. These learning will help the attacker the datasets which is overlap with training target data and motive of this unsupervised learning is not to identify the score of data point in D will represent the embedding in space, which helps to separate the active nodes from an inactive node using clustering algorithms.

Let x be the data points, which is targeted by the attackers or illegal users to determine the data points. Let us assume the attacker is one of the participants. The attacker runs a gradient ascent on x, and update the local model parameters in the direction of increasing the loss on x. This can simply be done by adding the gradient to the parameters by following equation,

$$W \leftarrow W + \gamma \frac{\partial L_x}{\partial W'} \quad \text{.....(3)}$$

The proposed scheme consists of the following few algorithms:

[1] ***Setup (K):*** The system setup algorithm takes a security parameter, K, as input. It outputs the public key (PK) and the master key (MK).

[2] ***Create attribute authority (PK, AA):*** This algorithm is executed by the GA (central authority) with the AA request as input. It outputs a functional identifier, Aid, for the AA with a set of attributes, Sid, and a secret authority key, SKA id. The Ministry of Health categorizes the AAs according to their functionalities and then assigns the attributes for users of these functionalities.

Attribute Key Generator (PK, SKA id, Sid): This algorithm is executed by the A id domain authority. It takes input PK and the domain authority secret key (SKA) id, the set of attributes S id. Outputs of the attribute secret keys for the user, will encrypt the texts (PK, M, P, PKU). The encryption algorithm take input as PK, and message as M and the set of public user keys (PKUs) corresponding to all the attributes in P. It outputs the ciphertext message CT.

Decrypt (PK, CT, P, SK Uj, SKA): The decrypt algorithm takes input PK, a cipher text message CT, the same access P used in encryption, the secret user key SK Uj and the set of secret attribute keys. The CT message will be decrypted if the attributes are sufficient to satisfy the P otherwise, the output will be null.

3.4. Evaluation metrics

i. ***Accuracy:*** the execution of model has two different classes as active member and inactive members. The illegal attack accuracy is the outcome of legal member with proper predictions with unknown data points. The size of data points is evaluating the illegal attacks.

True positive & False positive: it will provide more detailed performance of model by measuring the true positive and false positive rates, where the positive is associated with illegal output of inactive nodes.

iii. ***Prediction model:*** for classification model, prediction uncertainty is calculated using the normalized entropy of prediction for given input as given equation below,

$$H = \frac{\square}{\square\square\square(\square)} \sum_{\square=\square}^{\square} \square\square\ \square\square\square(\square\square) \ldots\ldots\ldots\ldots (4)$$

3.5 K- Anonymity algorithm:

In context of k- anonymization issues, the database is a table contains the n rows and m columns where the row of a table represents the record of patient details with their medical history as well as doctor details who is handle the certain patients with their specialization. All the rows and columns should be unique to avoid the data which is repeated randomly by occupying the additional space. The values in different columns are considered as attribute values which is associated with patients record and doctor's details.

The below table shows the data of non- anonymized datasets consisting of patients record with some hospital local database.

Table 1. Non- anonymized database about patient medical history from private hospital in Coimbatore district

TId	User Id	Prescription	No of Tablet	Morning	Afternoon	Evening	Night
TKID1006	UID1001	CROCIN	6	Select	Select	Select	Select
TKID1006	UID1001	CROCIN	6	Select	Select	Select	Select
TKID1006	UID1001	CROCIN	6	Select	Select	Select	Select
TKID1006	UID1001	CROCIN	6	Select	Select	Select	Select
TKID1006	UID1001	CROCIN	6	Select	Select	Select	Select
TKID1001	UID1002	CROCIN	1	Yes	No	No	No
TKID1001	UID1002	paracetamol	1	No	No	No	Yes
TKID1001	UID1002	metacine	1	No	Yes	No	No
TKID1001	UID1002	paracetamol	1	No	No	Yes	No
TKID1001	UID1002	CROCIN	1	No	No	Yes	No
TKID1002	UID1002	CROCIN	1	Yes	Select	Select	Select
TKID1002	UID1002	paracetamol	1	Yes	Select	Select	Select
TKID1002	UID1002	paracetamol	1	No	Yes	Select	Select
TKID1002	UID1002	metacine	1	Select	Yes	Select	Select
TKID1002	UID1002	CROCIN	1	Select	Yes	Select	Select

This algorithm performs the group-based anonymization and it is susceptible to many attacks when the knowledge is openly available to attacker, such illegal attacks are effective. Some possible attacks are given below,

1. Background knowledge attack: it associates the values between more than one attributes with sensitive data for reducing the set of possible values for sensitive attributes.
2. Homogeneity attacks: the entire sensitive values within the set of k records are simply identical and the data is k- anonymized with the sensitive value from the database are exactly predicted.

K- anonymity Algorithm:

Input: datasets with r tuples

Start

Step 1: attribute recognition (identifier, sensitive attributes, numeric and non- numeric values).

Step 2: eliminate the identifier attribute.

Step 3: sorting attributes.

Step 4: recognize the class and groups from the database.

Step 5: create an equal/ unequal grouping for generating the sub database.

$$IL(\gamma) = \sum_{i=1}^{p} IL(\sigma i)$$

4. Results & Discussion

This section discussed about the data privacy of health care industries using their own private cloud with federated learning method and centralized techniques. The patient history of certain hospital will be taken as input data and individual cloud has created for individual health record maintenance. Individual patient registration and their health issues related data are surveyed and stored in the local cloud. The followings results explained about the federated learning method of creating the individual registration for patient and doctor to maintain the individual record for faster treatment of patient's using local cloud databases. Individual registration of doctor and patient are created and maintained by the admin user to handle entire process using local cloud storage. The admin will create patient and doctor login by using attributes like name, age, mail ID, address, etc., to create individual local host page for future access in faster way. Medical history of individual will be recorded and make it private using key generation method for protecting patient details from the unauthorized or illegal access of the data or information.

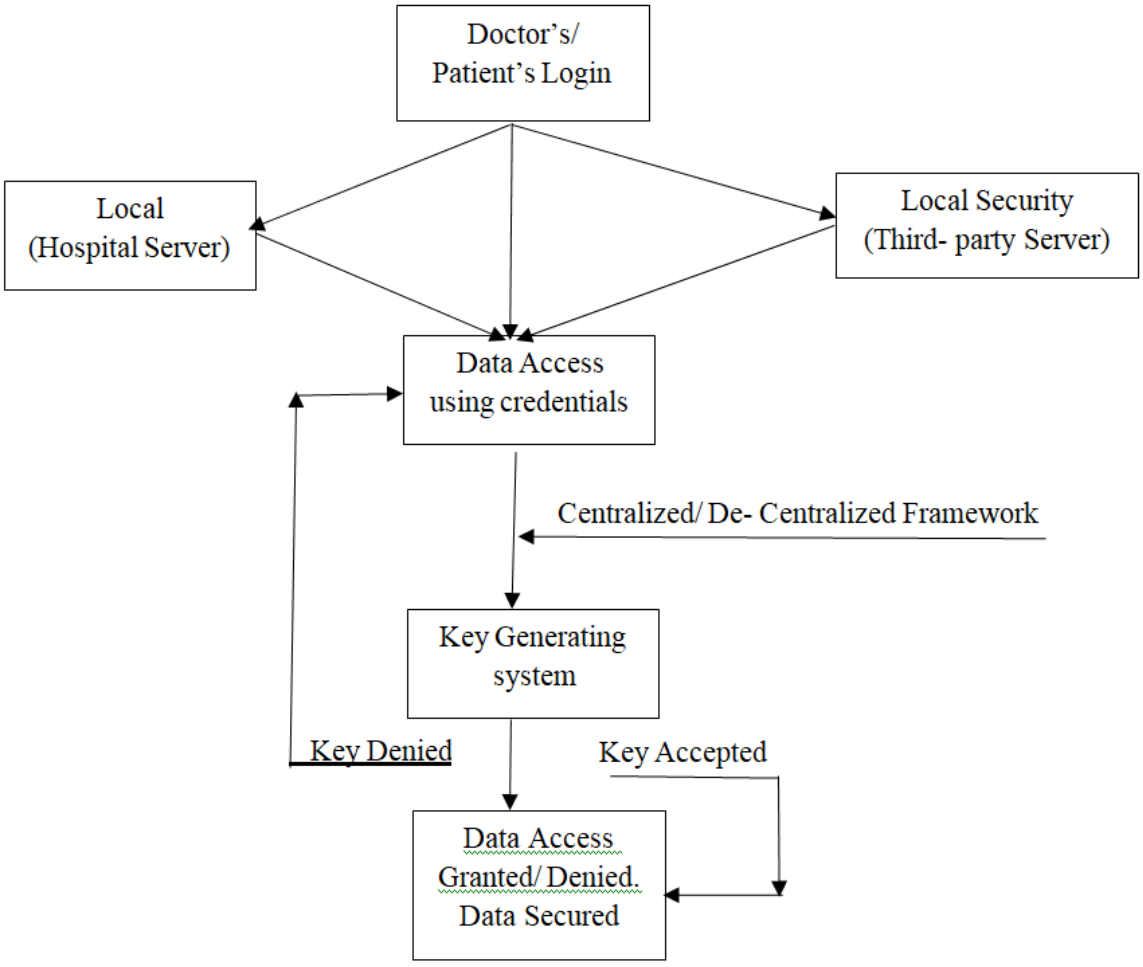

Fig. 2: Block diagram of proposed work

User have to login into their respective local host to access their own data and manipulate the data if requires. All the recorded data will be converted into word or excel file format for easy transfer to the users (Patient's) by doctors using highly impacted privacy.

The registration class diagram of patient and doctor using some selective attributes to register in the closed local hosts. The security of the local server has enhanced and protect the user's information from illegal access. It has a type of converting the data file from excel-to-excel formatted file for easy access.

Admin has created a local host for monitoring the health data about the patient and doctor who handle the patient's history login available. This page will consist of two major tabs as login and registration options for registration of patient details and creation of doctor's login. The login page for individual user's given for private access of data from the server. The patient's registration details here as token information as selective parameters such as token id, user id, name of patient, doctor whom the user consults, reason for consultant and date. All the medical history about the patient and handler information are provided.

The e- medical prescription of patient about the drugs to take at which time what are the drugs suggested to the patients by doctors for their health- related issues are displayed and the registration of doctors in cloud database with attributes id, name, DOB, age, address, specialist, experience and which hospital they working. Every doctor in the hospital should register their details in a local server database for easy access and safely protected their information using centralized and decentralized method with federated learning method.

4.1. K- anonymity algorithm:

The proposed model will train the data of patients using K-anonymity algorithm and identifies the member and non -member instances from the database as mentioned below in figure.

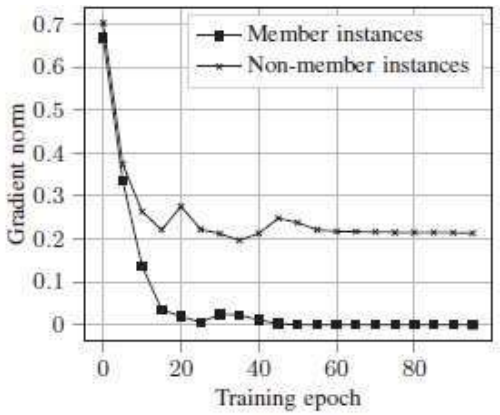

Fig. 3. Learning epoch for identifying the member and non-member instances from the database

The proposed model implements and compare the performance analysis with various models and train the supervised and unsupervised models with different datasets based on the testing and training datasets size. The proposed model with N number of datasets is compared using training sizes and executed without any overlap among the comparison of training sets of data. We train the proposed model with 25,000 instances overall for comparing the members and non- members instances among the databases contains 34,000 instances.

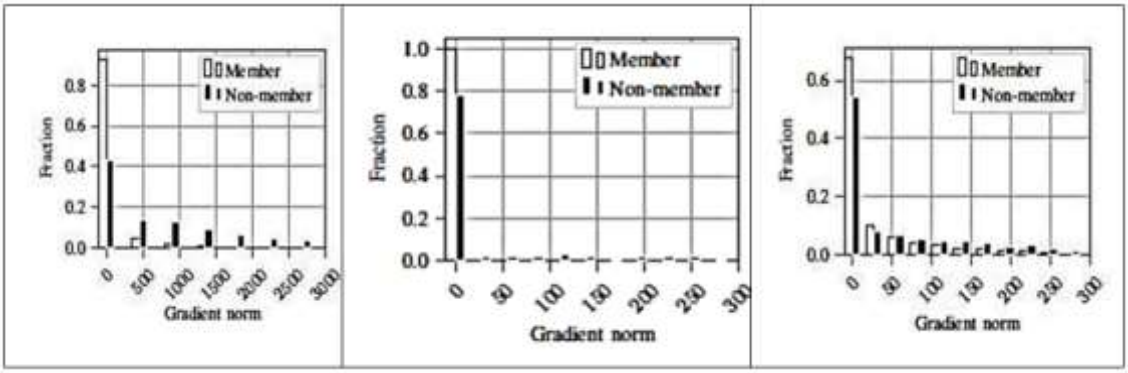

Fig. 4. Gradient norms distribution to identify the member & non- members instances from different pre- trained models (AlexNet, Densenet, Resnet).

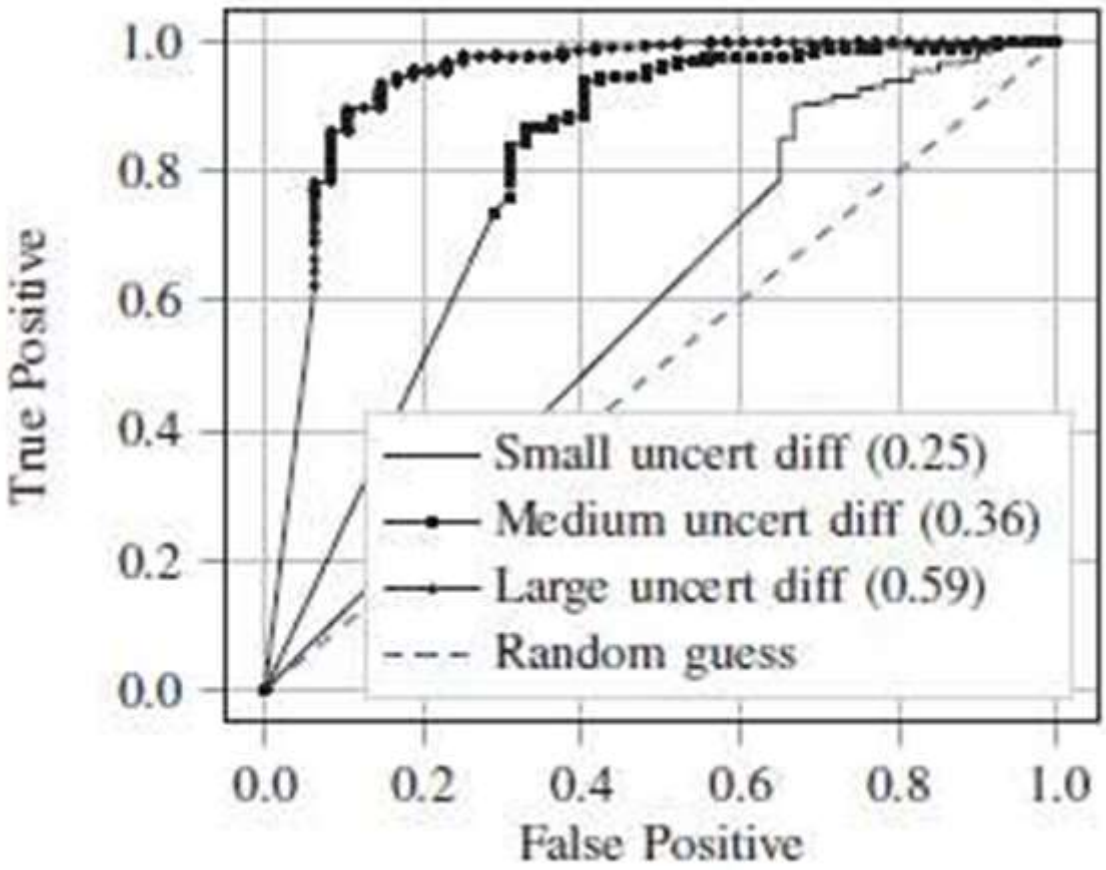

Fig. 5. ROC for the data with different prediction values using federated learning models

The below figure 7 shows the l diverse model that suggest the methods to overcome the troubles by altering the privacy of user which requires the diversity in class values for each tuple of the datasets and the proposed algorithm is altered to enforce the entropy value by checking the overall tuples in a database to calculate the entropy for comparison with threshold of log (l). This method helps to show the best level of diversity when there is similar chance to get each class values with no classification ability, therefore, the parameters of k- anonymity and l- diversity are not comparable

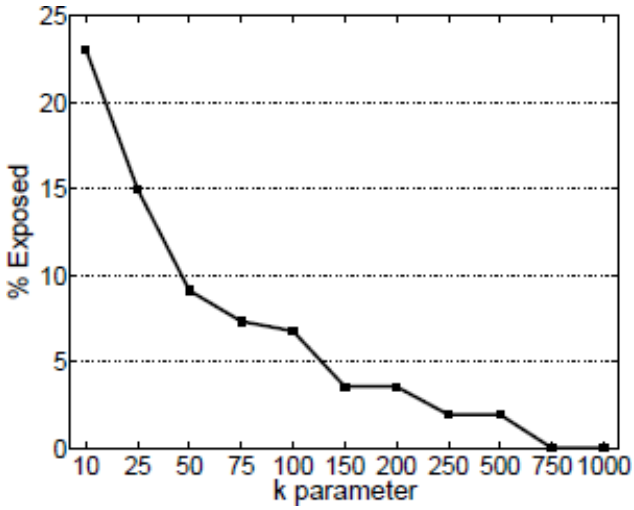

Fig. 6. Percentage of tuples from the database

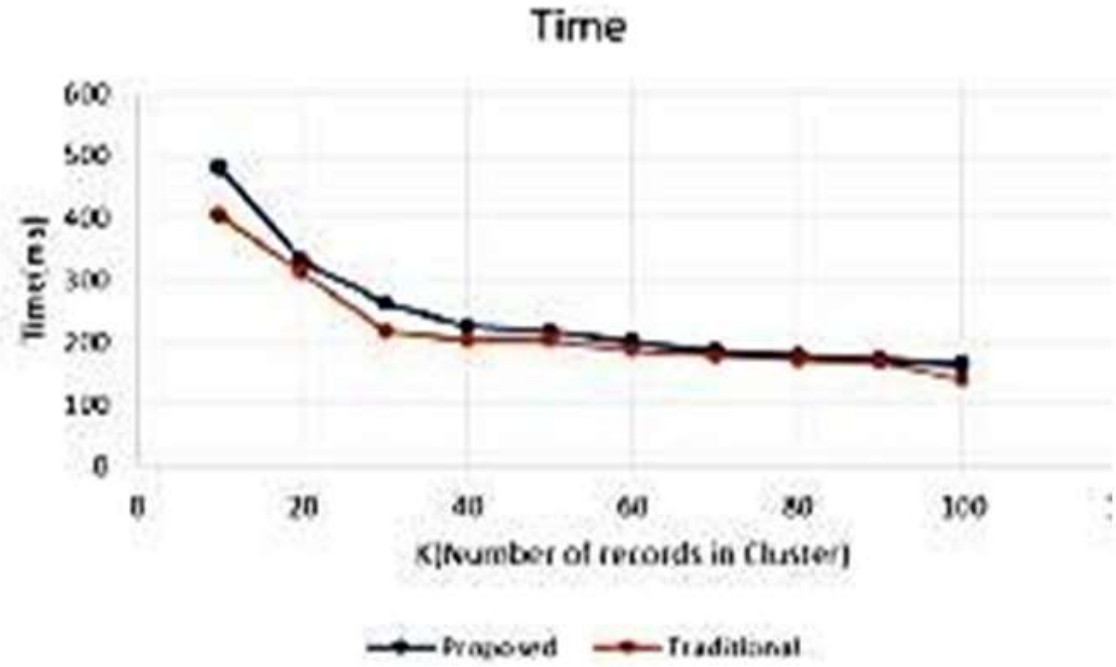

Fig. 7. Accuracy of proposed model

An execution time of proposed system with different values of patients from the local database decreased by the system than existing model. The proposed model takes time for execution than 2 level K- anonymization approach which executes the best due to fewer loss of information from the database of hospitals. The accuracy predicted for proposed model by preserving the user data of certain database is found to be 94.86% by comparing with existing model executes 86.98%.

5. Conclusion

In this paper, we proposed a secure cloud- based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-

authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no computational overhead is completed by the government authority, and multifactor applicant authentication have been identified and proofed.

The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment as future enhancement.

Acknowledgement
There is no funding support for this research from any institutions and not from any funding organizations of private or government bodies.

Conflict of interest
There is no conflict of interest.

References

[1] David Byrd, et.al., "Different agent simulation of marketing with high fidelity", published in conference proceedings of ACM, Principles of advanced discrete simulation, pg.. 11–22, 2020.
[2] C. Dwork, A. Smith, "Traceability of data with trace amounts with robustness" Foundation of Computer Science (FOCS), 56th Annual Symposium on. IEEE, pp. 650–669, 2015.
[3] Shokri, et.al., "Membership of various attacks using machine learning models," conference of Security and Privacy, IEEE Symposium, 2017.
[4] Fred, et.al., "Machine learning methods to analyze the risks of privacy" Computer Security Foundations, IEEE Symposium, 2018.
[5] Bacon, et. al., "Model to improve the communication efficiency using federated learning methods, 2016.
[6] S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770–778, 2016.
[7] G. Huang, Z. Liu, "CNN connected layers with dense net." Journal of CVPR, vol. 1, no. 2, 2017.
[8] C. Zhang, et.al., "Understanding the deep learning requirements for generalization", 2016.
[9] Long, et. al., "Learning generalized model for understanding the membership of inferences", 2018.
[10] A. Salem and M. Backes, "Model and data independent membership inference

attacks and defenses on machine learning models,"2018.
[11] H. B. McMahan, et al., "Communication- efficient learning of deep networks from decentralized data," arXiv preprint arXiv:1602.05629, 2016.
[12] M. Abadi, L. Zhang, "Deep learning model for enhancing the data privacy," Proceedings of ACM, SIGSAC Conference on Computer and Communications Security, pp. 308–318, 2016.
[13] R. Shokri, et. al., "ML model to protection of data using federated model," Proceedings of ACM SIGSAC Conference on Computer and Communications Security, pp. 634–646, 2018.
[14] J. Hamm, "Machine learning scheme to preserve the privacy of data from attacks," Journal of Machine Learning Research, vol. 18, no. 1, pp. 4704–4734, 2017.
[15] Rajagopal, "Generative adversarial privacy," arXiv preprint arXiv:1807.05306, 2018.
[16] M. Fredrikson, et.al., "Model inversion attacks that exploit confidence information and basic counter measures," Proceedings 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1322–1333, 2015.
[17] N. Carlini, and D. Song, "The secret sharer: Measuring unintended neural network memorization & extracting secrets," arXiv preprint arXiv:1802.08232, 2018.
[18] F. Zhang, Reiter and T. Ristenpart, "Stealing machine learning models via prediction apis," USENIX Security, 2016.
[19] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," arXiv preprint arXiv:1802.05351, 2018.
[20] L. Wei, et.al., "I know what you see: Power side-channel attack on convolutional neural network accelerators," arXiv preprint arXiv:1803.05847, 2018.
[21] L. V. Mancini, A. Villani, D. Vitali, and G. Felici, "Hacking smart machines: How to extract meaningful data from machine learning classifiers," International Journal of Security and Networks, vol. 10, no. 3, pp. 137–150, 2015.
[22] Reza Shokri, and Vitaly, "Membership inference attacks against machine learning models", In 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 3–18, 2017.
[23] Milad Nasr, Reza Shokri, and Amir, "Comprehensive privacy analysis of deep learning: Stand-alone and federated learning under passive and active white-box inference attacks", arXiv preprint arXiv:1812.00910, 2018.
[24] Peter, et al., "Advances and open problems in federated learning", arXiv preprint arXiv:1912.04977, 2019.
[25] Vladimir Ivanov and Aaron Segal, "Practical secure aggregation for privacy-preserving machine learning", In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 1175–1191, 2017.
[26] Ben, H Brendan McMahan, Aaron Segal, et.al., "Security model for privacy preserving using machine learning techniques", Proceedings of ACM SIGSAC Conference on Computer and Communications Security. ACM, 1175–1191, 2017.