IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115219

A Deep Learning Based Proposed Framework of Privacy Preservation in Cellular System

Shafiq Hussain [1], Chin Yen [2]

Chenab Institute of Technology, Gujarat, India[1]

Nanjing Institute of Information Technology, Nanjing, China[2]

Abstract: Now a days the obtainability of smart Phones, cameras and sensors are highly increased and becomes the important part of our daily life. Due to the usage of these devices huge data is produced and is placed on local platform. Local platforms are not able to perform exhaustive calculations. Cloud services are used for storing huge data that is produced from mobiles, sensors and cameras.

Advances in machine learning and computer vision provide huge cloud services with ability of content analysis and many other facilities. But suffers from unwanted privacy risks to users or individuals. In this paper our major focusing point are the privacy preserving techniques we proposed a hybrid framework also feature extractor and classification approaches for machine learning. Noise addition feature is also use to enhance security. Our proposed solution reduced the privacy ricks.

I. INTRODUCTION

The increased accessibility of connected devices like smart phones, cameras and sensors plays a major role in our daily life and also becomes the important part of our life[1,2]. The usage of these devices produced a huge amount of data. Handling this large amount of data at local Platforms is very problematic because local platforms are unable to perform exhaustive calculations. Majority use cloud services to handle this huge amount of data. People collect data from different devices which are in different forms and transfer it on the cloud to get benefits from the cloud services. cloud provide many services to the users but when people shift their data on cloud they have no more control over data and suffer from the privacy risks. Privacy are the major issues because the huge data may contain users personal identity, health record etc. To protect user data privacy different schemes were proposed.

Throughout the paper we are proposing a hybrid framework for protecting user privacy for data. We achieve a compromise between the local platforms and the cloud services.in our proposed solution local platforms and the cloud system collaborate with each other to accomplish a chore.in our proposed system we use two modules: feature extractor and other is classifier.

Features extractor is used at the client side which excerpt the private features from the data.Classifier module is at the server side which receive the private features and process them.to increase the privacy noise addition, Siamese Fine-tunning, Dimensionality Reduction are also used. We start by introducing a hybrid framework which address the data privacy problem. We use deep neural networks and divide the layers into two portions: feature extractor and classifier. Our proposed method reduced the privacy risks. We produced this through different experiments.

RELATED WORK

User data privacy is the major issue.to solve the privacy issue different method are proposed. A method of Differential privacy is proposed to solve the privacy problems.in this method privacy can be achieved by adding noise[3]. Drawback of this technique is that it only prevent from gaining additional information from an individual data. Non- invertible linear transformations and non-linear transformations are also proposed to solve the privacy risks.

Linear transformations provides the privacy protection at limited scope. While non-linear transformations technique use the minimax filter. This scheme provide better privacy protection but this privacy protection is only for Interpretation phase. By using this scheme privacy protection between cloud and local platforms is difficult to control. Some cryptographic techniques also used to protect data. Some people proposed by increasing the extent of ambiguity in the data privacy can be accomplished.

Also to protect image privacy different scheme are proposed that the face in an image do not recognized by face recognition system. Visual filter and morphing techniques are used for this perseverance. But these methods not provide privacy assurance for new models.

In machine learning and neural networks harmonic encryption techniques are also used to protect user privacy[4]. All the previously proposed methods are not suitable for high-dimensional data like multimedia. Also all these methods are not

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115219

reliable for different attacks. Our proposed method a hybrid Framework for Privacy Protecting Mobile Systems solve the user data privacy problems.

II. METHODOLOGY

A Hybrid Framework:
We present a hybrid framework for privacy protecting mobile system.in this frame work local platforms and cloud systems collaborate with each other to perform task. This framework contain two Modules:

- Feature extractor
- Classifier

Feature extractor:
This module is at the client side and abstract the isolated information from the user data. The feature extractor module firstly acquires the input data and activates algorithms on it and gets new feature vector from it.

Classifier module:
Classifier module is at the server side which receive the private features and process them.
In our proposed framework the user and the service provider collaborate with each other to perform tasks. The user use the feature extractor module and extract the private features from the data. Remove all the sensitive information from the data and keep only necessary information that is relative to primary measures. Then the user transfer the data on cloud. Now the service provider determine how the user extract the private features. Also the service provider use the classifier module receive data from user and perform further processing.
In our proposed framework the major challenge is how to design a feature extractor module. Because this module perform major task. This module eliminate all the sensitive information .sometimes by removing delicate information some crucial information may lost so designing of this module is a big challenge.in our framework.
We propose a novel method to embed a feed forward neural network and design a feature extractor module. Also verify the privacy of this module by using different methods including privacy metric.

Deep Privacy Embedding:
In mobile analytics the admiration of deep learning are highly increased. Deep neural networks also have high popularity in data mining and machine learning applications.
In our proposed method we use a deep neural network (DNN) due to their increased popularity in mobile analytics. In this segment we govern how to entrench a pre- qualified deep neural network in our framework. Complex deep neural network has many layers .By using layer mechanism we entrench these layers in our framework.
In our framework we choose the middle layer as a pivot point and divide the whole frame work into two parts. Layers above the pivot point are called upper layers and the layers below the pivot point are called lower layers.
The first part contain the upper layers and forms the feature extractor module. The second part contain the lower layers and forms a classifier module.so by using layer separation mechanism we obtain a feature extractor module and also gets reimbursements from the deep models.by using this deep embedding when we move towards the deep layers privacy can be achieved.by using higher layers as a middle one the more processing of data is on the user device and privacy of user data can be achieved.at end we apply three different techniques:

- Siamese Fine-tunning
- Dimensionality Reduction
- Noise Addition

Siamese Fine-tunning:
This structure has been used to verify the applications for a very long time. The main idea was to represent two of similar points to come closer to each other and two different orients to make them away. Dissimilar distance is calculated and defined in a way to make them maximum and minimum for same points. The function we use is
$L(f1, f2) = ||f1 - f2||^2$ similar $\max(0, \text{margin} - ||f1 - f2||)^2$
dissimilar
Here, f1 and f2 are mapping points of data. It is not designed for classification, it works in a scenario. To create a face representation we use a deep model having a layer of softmax in conclude.
In kernel, pictures of same personality are near to each other. In test phase, only one side of network is sufficient due to same parameters to achieve privacy preservation objectives.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115219

The main concept is of k-anonymity. Actually, our intention is to build an approach to generate many to one substances/objects with CT1 class and different CT2 class. Defining similarity is on base on CT1. Similarly, image with same emotions are categorized in one class and dissimilar emotions are categorized in different class.

Dimensionality Reduction:

Service providers collect immediate features from Siamese structure and apply PCA on them. They choose k as dimensional number and give projection matrix to k toward the peregrine client.

The user use this estimate to reduce feature size then send to server. Server knows the matrix and can reconstruct the reduced features based on PCA eigenvectors. This reduces common cost.

Noise Addition:

After reducing features, Gaussian noise is added. After this Siamese network give k- anonymity and map vary objects from same class to same points in feature zone while in reality these orients have similar orbit between them. Comparison of distance is not effective and uncertainty is much challenging.

Feature Extractor Validation:

For authenticity of the level of secrecy of feature extractor noise is applied to immediate features. We estimate likelihood of each CT2 class. For this we calculate P(z|ci) in this way.

$$P(z|c_i) = \int_X P(z,x|c)dx$$

$$= \int_X P(z,x,ci)P(x|ci)dx \quad (2)$$

Conditioned on x,ci is independent od z,so we have:

$$P(z|c_i) = \int_X P(z,x|ci)dx$$

$$= E_x \sim P(x|c_i)\,[P(z|x)] \quad (3)$$

Assuming $X_i = \{x1,x2,\ldots..xN_i\}$is the set of points

Emotion Detection:

From facial expression the detection of emotions is becoming important. On basis of different facial expressions emotions are classified. We use VGG-S-RGB model having VGG-S format and deep pattern of 8 layer for categorization of image. Accuracy is 39.5%.

Experiments:

In experiments we check the validity and privacy of different embedding in different layers. We proof how simplification of dimensions results positively on secrecy. Then we will check our core on the mobile phone and its benefits according to other results.

Interpreting the Gender Categorization:

We impose privacy mensuration on vary medium layers of gender categorization and patterns of face recognition, to represent the privacy of our format. We apply the VGG- 16 pattern suggested in simple embedding.

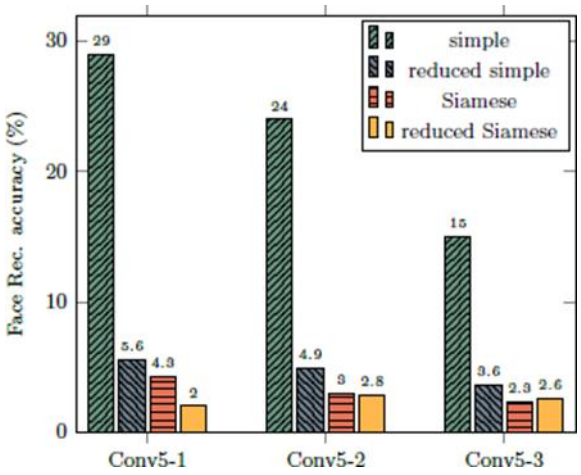
For obtaining Siamese embedding, we apply a pre-trained system of connections. We impose PCA on intermediate characteristics of the simple embedding and the Siamese embedding, severally.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

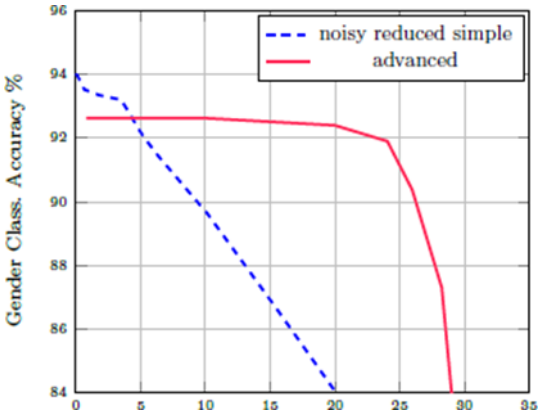
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115219



Efficiency of the actual face recognition is 75%.Conv5-1 severally

The motivation of this tendency is arise straight the layers. Face Recognition validity is less than the accuracy of simple embedding. Reduce simple and Siamese has low face recognition accuracy[5-9].
To judge extent of these changes affect authenticity of required task that is gender division, we note varying embedding validities. Siamese embedding is more robust to PCA.
Gender categorization authenticity of lessen Siamese embedding is near to the actual Siamese embedding, while the reduction of dimensions effect badly the correctness of the simple embedding. To authenticate feature extractor, rank measure is used. When we increase variance of noise, we obtain high privacy and low correctness.
Service provider gives gradually bending line of accuracy-privacy (like following Figure) and we obtain similar result with that type of privacy mensuration (Separate of face recognition pattern). VGG-16 structure increases more slowly in advanced embedding than other embedding[10].



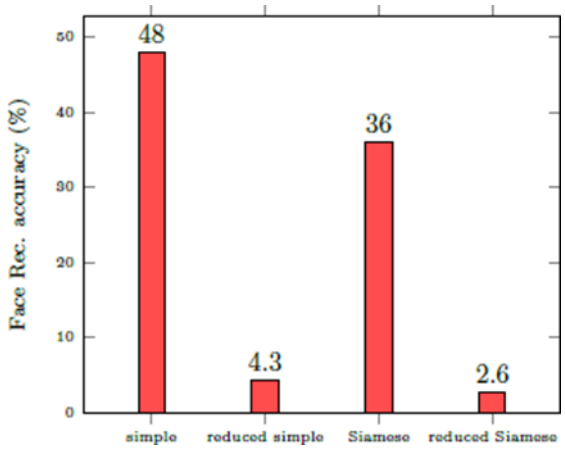
Evaluation of motion detection:
To check the framework for task of emotion detection, CT1 refer as the emotion detection and CT2 as the face recognition. We are using the VGG-S RGB, pre- trained network. We fine tune model and obtain Siamese embedding. VGG-S has the smaller architecture in contrast with VGG-16 (8 layer vs. 16 layer), we compare embedding upon the layer that is Conv5.
The correctness of the face recognition model is less for all embedding. The Siamese embedding helps with privacy protection. Siamese embedding do not lessen emotion detection's efficiency prominently, while dimensionality reduction has a great effect on this task.
Through rigid correctness level, there is higher privacy for the progressing embedding. Result shows that format is application independent and also model independent. The Siamese architecture amends privacy, while reduction of the dimensionality does not affect CT1 authenticity and reduces the cost of communication. We use the authentication method to quantify level of privacy, and no access is given to the cloud-based pattern of face recognition.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115219



Mobile Evaluation:

In the deep network, parameters in the whole connected layers are many more than the parameters of convolutional tier. In the framework, few convolutional tiers are applied on the mobile, this resulting a considerable decrease in the model initialization time and consequently power consumption.

We use Cloud for the conclusion phase, so the only chokepoint is putting input through the convolutional tier that are located upon the mobile. Many vary procedures like specification and compression also attempt to lessen convolutional layers cost of applying and also utilizes in the framework. Most of the fluctuations under the proposed embedding method of the trained model structure has the similar runtime efficiency.

III. CONCLUSION

We showed an advanced hybrid framework for effective privacy protecting on the mobile systems. The proposed framework include a classifier and a feature extractor, where the feature extractor is located at client side and the classifier at server side.

We sink the convolutional neural networks in our framework to get advantage from their authenticity and layered structure to preserve the privacy of the data.

We utilized the Siamese framework. To remove the unwanted data from the drawn out feature concludes the accomplishment of secrecy for users. We evaluated our framework by partitioning the layers in to the cloud and mobile and also through the noise addition. And we accomplished more accuracy in our required tasks.

REFERENCES

[1] Heydari.M, Lai.K.K, and Xiaohu.Z ,(2019) Risk *Management in Supply Chains: Using Linear and Non-linear Models*. Routledge.https://doi.org/10.4324/9780429342820-5

[2] Heydari.M, Lai.K.K ,and Zhou.X,(2020)‘Creating sustainable order fulfillment processes through managing the risk: evidence from the disposable products industry,’ *Sustainability*, vol. 12, no. 7, p. 2871. https://doi.org/10.3390/su12072871

[3] Bansal.T,Gunasekaran.K,Wang.T ,Munkhdalai.T , and McCallum.A, (2021) ‘Diverse distributions of self-supervised tasks for meta-learning in NLP,’ *arXiv preprint arXiv:2111.01322.* https://doi.org/10.18653/v1/2021.emnlp-main.469

[4] Kommaraju et al.V,(2020) ‘Unsupervised pre- training for biomedical question answering," *arXiv preprint arXiv:2009.12952.* https://doi.org/10.18653/v1/d19-5823

[5] Bibhu.V, Salagrama.S ,Lohani B.P , and Kushwaha P.K., (2021)‘An Analytical Survey of User Privacy on Social Media Platform,’ *in 2021 International Conference on Technological Advancements and Innovations (ICTAI), 2021:* IEEE, pp. 173- 176. https://doi.org/10.1109/ictai53825.2021.9673402

[6] Salagrama.S, “(2021) ‘An Effective Design of Model for Information Security Requirement Assessment,’ *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10. https://doi.org/10.14569/ijacsa.2021.0121001

[7] Trapit Bansal, Karthick Prasad Gunasekaran, Tong Wang, Tsendsuren Munkhdalai, Andrew McCallum (2021), ‘Diverse distributions of self-supervised tasks for meta-learning in NLP,’ arXiv preprint arXiv:2111.01322.https://doi.org/10.18653/v1/2021.emnlp-main.469

[8] Karthick Prasad Gunasekaran, B Chase Babrich, Saurabh Shirodkar, and HeeHwang(2023),“Text2TimeTransformer

DOI: 10.17148/IJARCCE.2022.115219

based Article Time Period Prediction",ResearchgatePreprint, http://dx.doi.org/10.13140/RG.2.2.29195.36641

[9] Karthick Prasad Gunasekaran and Nikita Jaiman(2020), "Text2Time: Transformer-based Article Time Period Prediction", Researchgate Preprint, http://dx.doi.org/10.13140/RG.2.2.25839.92323

[10] Karthick Prasad Gunasekaran, Kajal Tiwari and Rachana Acharya(2020), "Deep learning based auto-tuning for database management system", Researchgate Preprint, http://dx.doi.org/10.13140/RG.2.2.21645.61920

[11] Karthick Prasad Gunasekaran (2020), "Ultra Sharp : Study of Single Image Super Resolution using Residual Dense Network", Researchgate Preprint, http://dx.doi.org/10.13140/RG.2.2.25001.06246