OFFLINE HANDWRITTEN SIGNATURES BASED MULTIFACTOR AUTHENTICATION IN CLOUD COMPUTING USING DEEP CNN MODEL

By

K. DEVI PRIYA * L. SUMALATHA **

* Department of Computer Science and Engineering, Aditya Engineering College, Surampalem, Andhra Pradesh, India.
** Department of Computer Science and Engineering, University College of Engineering Kakinada, India.

Date Received: Date Revised: Date Accepted:

ABSTRACT

Cloud Security is an important factor that influences the adoption of cloud applications into bank domains. Many researchers proposed secure authentication mechanisms based on the traditional factors, biometric factors, captcha and certificates etc. In this paper, proposes biometric handwritten signature recognition using Deep Convolution Neural Networks (DCNN). The proposed model uses signature as a biometric factor to verify the authenticity of the users along with traditional credentials. The extraction of the features are performed using DeepCNN model in the registration and verification process. The practical setup is done through NIVIDIA DGX environment using Python keras and tensor flow as backend. An experimental result shows 99% of accuracy and validation accuracy.

Keywords: Cloud Security, Handwritten Signatures, Convolutional Neural Network, Features Extraction, Cloud User Authentication, NIVIDIA DGX Python Keras.

INTRODUCTION

Cloud Computing is a technology that offers services to the users on request basis (Mell, & Grance, 2011). The services referred as SAAS (Software as a Service), PAAS (Platform as a service), and IAAS (Infrastructure as a Service) (Armbrust et al., 2010) With increasing popularity of cloud computing and flexibility offered, the transformation of the traditional banking adopts the cloud technology to offer services to the customers in a flexible way at low cost (Suresh, 2010). Bank organization use Cloud to provide effective, innovative services and speed up the transactions etc., of the customer's requirements (Yan, 2017). Despite the benefits of the cloud, the main problem associated with the cloud server and cloud banking is security (Carroll, Van Der Merwe, & Kotze, 2011; Hamidi, Rahimi, Nafarieh, Hamidi, & Robertson, 2013; Huang, Tzeng, Tzeng, & Yuan, 2011; Catteddu, 2009; Zissis & Lekkas, 2012; Rani & Gangal, 2012). Customers upload their personal details, documents into server and there is chance of theft of the data and documents by unauthorized users. Lots of research is done on cloud security in-terms of two-factor authentication, multifactor authentication, biometric authentication but still security is consider as open problem in the cloud computing (Adjei, 2015; Lee, Ong, Lim, & Lee, 2010; Choudhury, Kumar, Sain, Lim, & Jae-Lee, 2011; Banyal, Jain, & Jain, 2013; Jiang, Khan, Lu, Ma, & He, 2016; Liu, Uluagac, & Beyah, 2014).

The proposed algorithm uses bio-metric multifactor authentication that includes traditional userID, password along with the user handwritten signatures as a third factor (Trevathan & McCabe, 2005). The authentication parameters of the user are captured in the registration process and features of the signatures are extracted using Deep Convolutional Neural Network (DeepCNN) model that have more than one hidden layer to extract the features. The DeepCNN model captures three to four user signatures in the registration process for extracting the relevant features of the user signature. In the authentication phase, the user need to submit the

credentials, and signature then the model predicts the signature of the user is valid or not by verifying with the specified threshold value. If the signature is valid then the user is allowed for the accessing the services from the bank server otherwise the user is denied. The remaining of this paper is organized as follows: section 2 focus on the related work. The detailed proposed scheme described in the section 3 and section 4 describes our proposed method. Section 5 indicates the results of our experiments. Conclusion of the paper is specified in the section 6.

1. Releated Work

Several biometric authentication techniques are proposed recently based on finger print, voice and face recognition fusion using traditional image processing techniques (Lee, Ryu, & Yoo, 2002; Abozaid, Haggag, Kasban, & Eltokhy, 2019; Hossain, & Muhammad, 2015). Cloud assisted framework is proposed using face and speech recognition for health monitoring. LF extraction is used for the extracting speech features, HTD calculation and HD calculation for extraction of the speech features and classification is perform by SVM classification. In this, Gabor binary pattern extraction is used for extracting features of the face that includes multi scale Gabor and center symmetric local binary pattern. In the traditional image processing the users need to define explicitly the parameters for the features extraction. The accuracy of the model is based on the defined features that are based on the user knowledge. Face classification using SVM ensemble and face detection using skin illumination model is specified in (Pang, Kim, & Bang, 2003; Kumar, & Bindu, 2006).

Recent research focus on the Machine Learning and Deep Learning algorithms to extract the crucial features of the different biometric factors of the large dataset for faces, finger prints, iris, palm, signatures etc, (Sun, Wang, & Tang, 2014; Howard et al., 2017; Hu, & Chen, 2013). The features of the signatures extracted using Deep convolution neural networks to classify the genuine and forgery users (Rivard, Granger, & Sabourin, 2013; Eskander, Sabourin, & Granger, 2013; Bertolini, Oliveira, Justino, & Sabourin, 2010; Hafemann, Sabourin, & Oliveira, 2017; Sun, Chen, Wang, & Tang, 2014).

2. Proposed Methodology

Biometric Authentication system represents pattern recognition system based on the individual physical behavior. The behavior of the person is considered to be unique and can't be forged by others. The combination of biometrics with cloud computing improves the security and accuracy of the system. The proposed framework is designed to authenticate the bank users based on their hand written signatures with the deep learning technique. However, the extraction of features from the hand written signatures is a challenge task. There may be chance of the forgery by the malicious user. In this work, the feature extraction is performed using DeepCNN that employs the extraction of the features automatically and two types of the cloud infrastructures are adopted namely public cloud, and private cloud. In public cloud, the same environment is virtually shared by the multiple users, and the private cloud environment is designed to the specific organization needs. In the proposed work, the Bank Server (BS), user database and Cloud Manager (CM) are maintained at the private cloud which is very secure and the CAS (Cloud Authentication Server) is maintained at the public cloud.

Figure 1 shows the system architecture of the proposed framework that contains Bank User, Bank Server, Cloud Authentication Server and Cloud Manager.

2.1 Bank User (BU)

The BU is the one who wants to avail the banking services from anywhere through the application installed on the mobile devices. BU submits the required credentials to the bank server in the registration phase for the authentication.

2.2 Bank Server (BS)

The main objective of the BS is to maintain the services at private cloud server. The services of the BS are as follows:

- User activation and revocation
- Management of bank services
- Monitoring of user activities
- Defining roles to employees

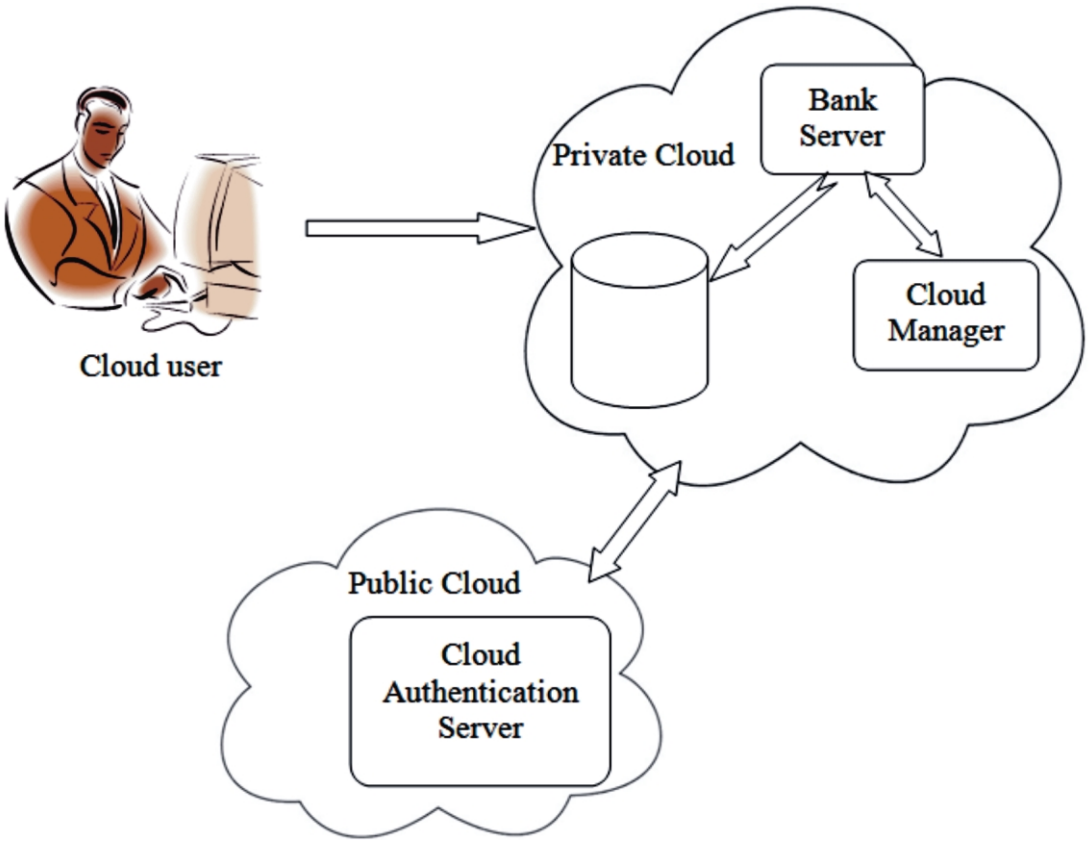

Figure 1. System Architechture

2.3 Cloud Manager (CM)

The CM is responsible for the maintaining the overall management of the proposed work in a secure way and the services are described below:

- Maintaining Virtual Machine VM
- Develop model for Handwritten signatures extraction
- Session Management
- Billing Service

2.4 Cloud Authentication Server (CAS)

The responsibility of the CAS is to authenticate the user authenticity. The CAS does not store credentials of the user at the public cloud. But it authenticates by using encrypted hash credentials (Nagaraju, & Parthiban, 2015).

The BU who wants to perform transactions, initially must be registered with the BS which is located at the private cloud. In the registration, the user must submit all the credentials required for the bank and chooses userID, and password to access the application. Once the userID is not registered earlier then the bank server requests the hand written signatures of the user. The user submits three to four offline signature images to the bank server and BS will store the signatures in the cloud database. The extraction of the signature features are performed using DeepCNN model. The performance and accuracy of the DeepCNN model is based on the hyper parameters and model tuning with different optimization techniques. Once the features are extracted the user state is set as active and ready for accessing the services. Steps of the registration algorithm is described in the below.

Algorithm 1. Registration

Input: userID, password, Handwritten Signatures

Output: Status of the registration

1. userID ← hash(userID)

2. password ← hash(password)

3. signatureImages [ ] ← preprocess (H_sign_Images)

4. BS ← send(userID | | password)

5. BS ← send(signatureImages)

6. save (signatureImages)

8. train_Images[ ] ← train (signatureImages)

9. Set_state (userID_active)

3. Deep CNN Model Features Extraction

The Convolutional Neural Network (CNN) model is inspired by multilayer perception model and is very useful for object recognition and classification. Several CNN models are proposed (Montserrat, Lin, Allebach, & Delp, 2017; Kuo, 2017; Strom, 2015). The performance of the model is based on the defined layers, parameters, training dataset and test dataset. The model used in our proposed work shown in Figure 2.

The building blocks of the DeepCNN model are Convolution layer, Pooling layer and dense layer.

3.1 Convolution Layer

The fundamental component of the CNN is Convolution layer that performs the feature extraction, which typically is convolution. Convolution is a specialized type of linear or non linear operation used for the feature extraction. This layer has the basic components like convolve, stride, padding, and activation function. The convolve function is defined with the parameters like number of filters and size of the weight matrix called kernel size or filter size. The filter size specifies the weight matrix of the image that is applied to the input image by moving the kernel over the image to get the convolved features. The movement of the kernel matrix over the input image is controlled by the stride. At each position, the number of values from the original image is multiplied with the number of the values in the weight matrix and performs the summation on all these values. The sum of this entire product is divided by the kernel normalizer.

The result is placed into the new image at the position where filter matrix is centered .Then the kernel is translated in to the next position of the original matrix and the procedure repeats until all the image pixels have been completed. In the proposed model the first layer is convolution layer with 64 filters and kernel size which is a 3x3 matrix with a non linear activation function Rectified Linear unit (ReLu).

3.2 Pooling Layer

The pool layer reduces the spatial dimension of the representation to reduce the number of the parameters and computation in the network. To perform the pooling different type of pool techniques are available consider as max pooling, min pooling and average pooling. The most commonly used technique is max pooling that picks the maximum value from the feature set matrix. The second layer defined in the model is max pooling with kernel size 3*3.

The above two layers are repeatedly connected to generate the accurate features.

3.3 Fully Connected Layer

In this layer, the fully connected layer have all the full connections to all the activations in the previous layer. This layer is defined using dense function with number of prediction classes. The most commonly used probabilistic function is softmax.

4. Login and Authentication

Authentication is the process that verifies the legitimacy of the user by validating the credentials. In the proposed framework, the authentication of the users is performed by CAS which is deployed in the public cloud. The CAS will perform the authentication of the users without storing the

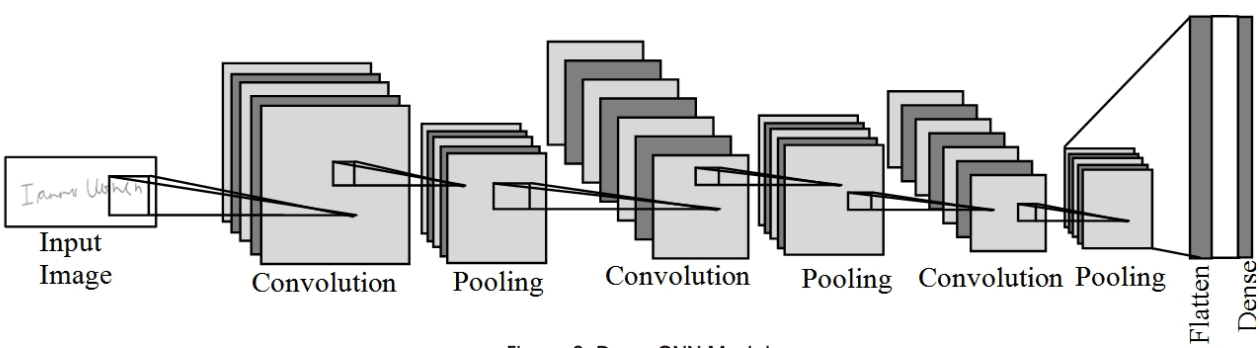

Figure 2. Deep CNN Model

credentials at the public cloud. For the authentication request, the user sends the encrypted hash based credentials to the CAS and CAS will keeps the encrypted password and send the userID to the bank server. Based on the userID the BS sends password to the CAS. The user performs the comparison on both user and BS hashed password if both are equal then it request the signature. The user sends the signature in a secure way and the CAS runs the model and calculates the score of the signature. If the score is greater than the specified threshold then the user is authenticated and allowed for accessing the bank services. The assumptions made in the proposed scheme is that the bank server services and cloud management is deployed in the private cloud and authentication of the users are done by the public cloud provider. The keys required for the encryption and decryption is exchanged by the trusted party.

Authentication is the process that verifies the legitimacy of the user by validating the credentials. In the proposed framework, the authentication of the users is performed by CAS which is deployed in the public cloud. The CAS will perform the authentication of the users without storing the credentials at the public cloud. For the authentication request, the user sends the encrypted hash based credentials to the CAS and CAS will keeps the encrypted password and send the userID to the bank server. Based on the userID the BS sends password to the CAS. The user performs the comparison on both user and BS hashed password if both are equal then it request the signature. The user sends the signature in a secure way and the CAS runs the model and calculates the score of the signature. If the score is greater than the specified threshold then the user is authenticated and allowed for accessing the bank services. The assumptions made in the proposed scheme is that the bank server services and cloud management is deployed in the private cloud and authentication of the users are done by the public cloud provider. The keys required for the encryption and decryption is exchanged by the trusted party.

Algorithm 2. Login and Authentication

Input: userID, password, Handwritten Signature

Output: Status of the user authentication

userID ← hash (userID)

password ← hash (password)

signatureImage ← preprocess(H_sign_Images)

$u_1 = (\quad)(E_{KU_{as}})(userID)||password))$

CAS ←Send (u_1)

D_{KR} (u_1)

Save password

$u_2 = (\quad)(\quad)(userID)))$

BS ←Send (u_2)

D_{KU} (u_2)

If (userID = = true)

$u_3 = (\quad)(BankServerID // password))$

CAS ← Send (u_3)

Decrypt (u_3)

Check if h (password') = h(password) if valid

CAS predicts the signature using CNN model

score ← Model·· predict (signature)

if score > = thresholdvalue

user is authenticated

else

user authentication failed

5. Experimental Results

5.1 Setup

The proposed model is simulated on NVIDIA GPU DGX system with the clock speed 1.5 GHZ and 16 GB RAM. The standard RSA asymmetric encryption algorithm used for the encrypting credentials for the exchanging process (Goud, n.d). The scheme is simulated using Python Keras and Tensor Flow as backend.

5.2 Database

The biometric handwritten signatures are collected from the dataset GDPS which is publicly available. Proposed model used 200 user's signatures collected in the registration phase based on the different writing styles. The model has taken 80% of signatures for the training and 20% of the signatures for test data set. The model observed 6,510,006 parameters as trainable

parameters. The model found10800 images belonging to 200 classes. The sample signatures of one user are shown in Figure 3.

5.3 Model Evaluation

To evaluate the performance of the CNN model for user authentication, the server runs the CNN model on training and test data set of all the users in the private cloud environment. The layers of the model are created using sequential model. The first layer of the model is convolution layer with 96 filters and kernel size is 11 x 11, stride value is 4 and kernel is initialized as Glorot uniform initializer. The activation output map of convolution layer is based on the parameters defined in the convolution layer. In the second layer of the model, batch normalization is applied with axis, momentum and epsilon parameters. The axis is an integer value for feature axis, epsilon value is a float value added to the variance for avoiding of division by zero and momentum value is used for moving mean and variance. The output of the previous layer is considered as input for the batch normalization and the shape of the output is same as the input shape. The pooling layer created as a third layer with the functionality max pooling with the stride matrix 2x2.Similarily, the above procedure is iterated with different layers with different filters and stride values. The second convolution layer is defined with 256 filters with stride values 1 x 1 and the max pooling layer followed by the dropout. Finally the fully connected layer created using dense layer with 128 nodes and then output classifier layer is created with signmoid activation function. To avoid the dead neurons Drop out with 0.3 value is applied. The Deep CNN is executed on the NIVIDIA DGX environment as shown in Figure 4 and the result screens are shown in the Figures 4, 5, 6, 7. Figure 4 shows the configuration details of the NVIDIA DGX GPU.

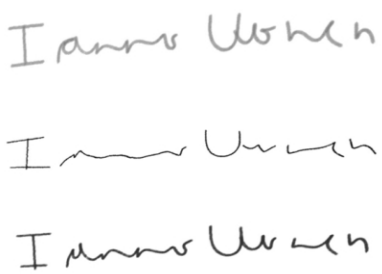

Figure 3. Sample Dataset of user1 from the GDPS

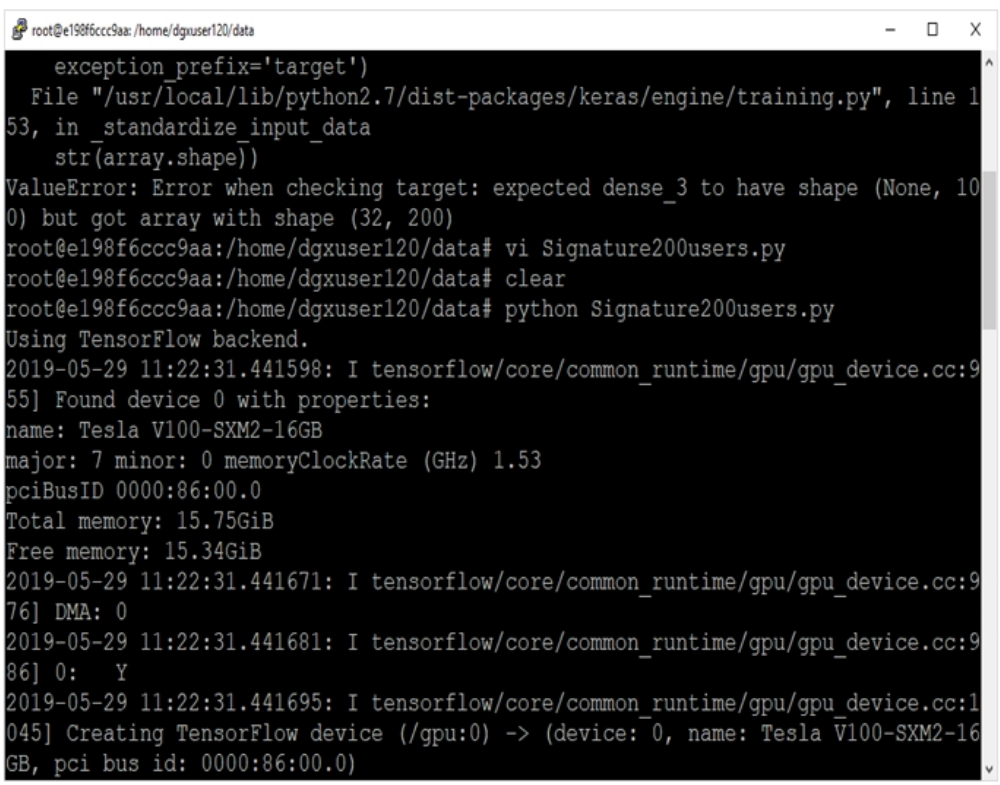

Figure 4. Model Configuration

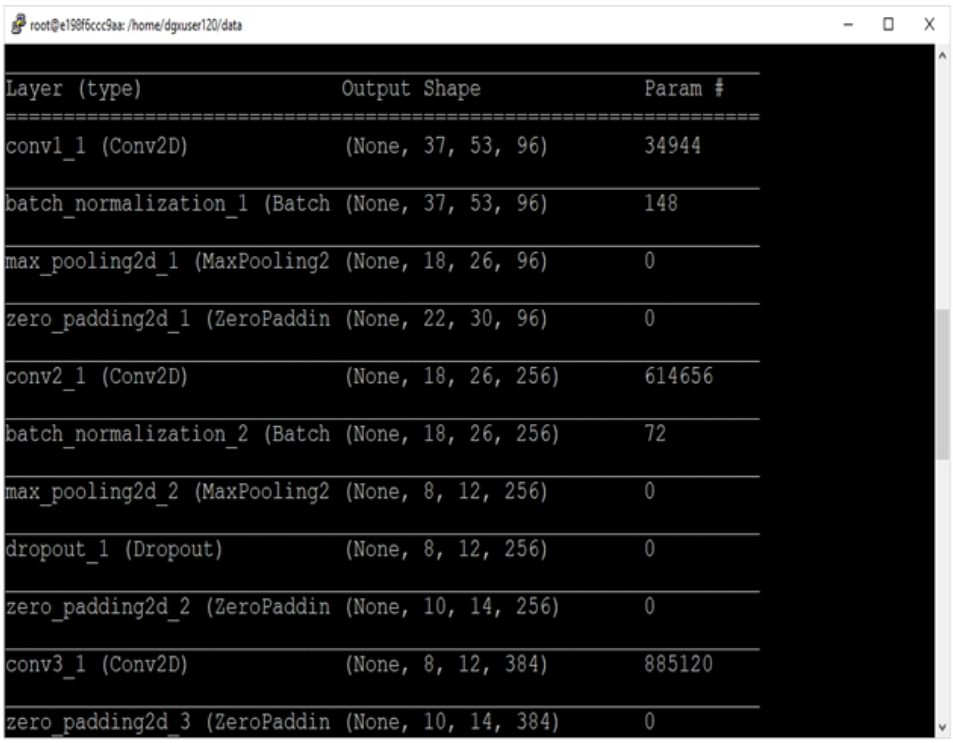

Figure 5. Model Summary

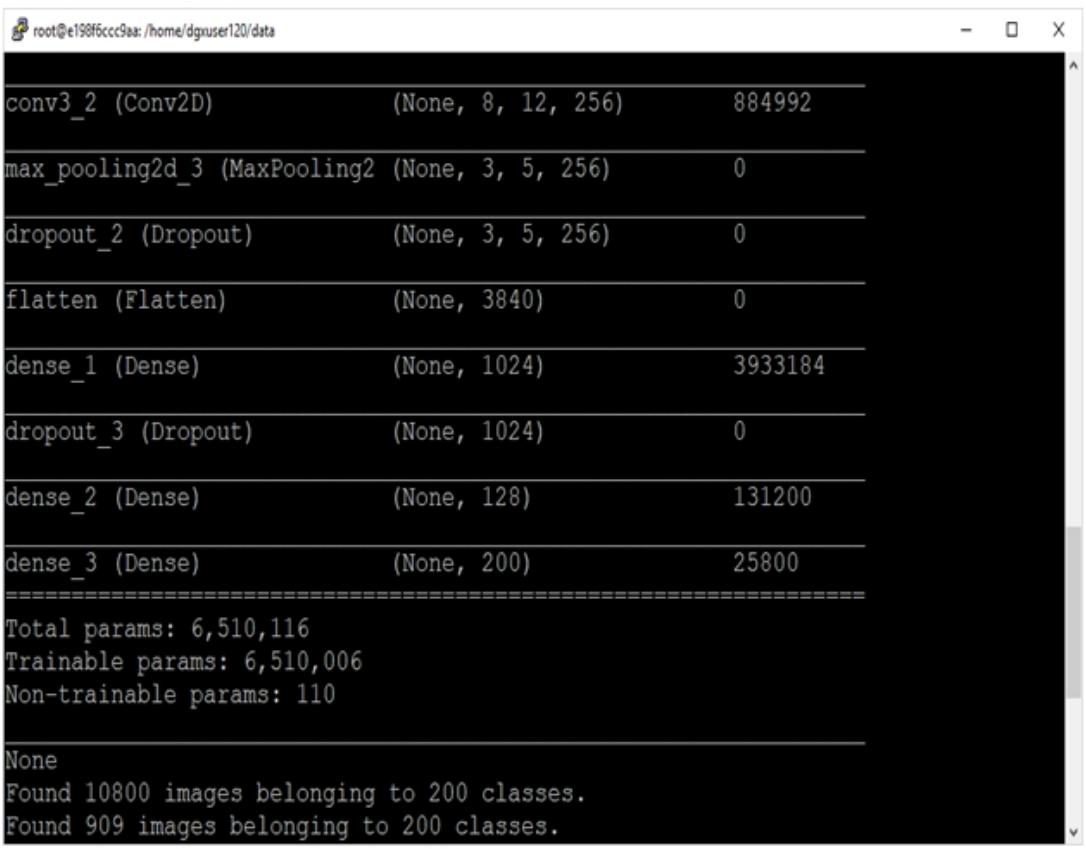

Figure 6. Model Summary

```
root@e198f6ccc9aa: /home/dgxuser120/data
Total params: 6,510,116
Trainable params: 6,510,006
Non-trainable params: 110
_________________________________________________________________
None
Found 10800 images belonging to 200 classes.
Found 909 images belonging to 200 classes.
Epoch 1/5
200/200 [==============================] - 68s 340ms/step - loss: 0.2351 - acc:
0.9828 - val_loss: 0.0524 - val_acc: 0.9950
Epoch 2/5
200/200 [==============================] - 63s 313ms/step - loss: 0.0423 - acc:
0.9950 - val_loss: 0.0361 - val_acc: 0.9950
Epoch 3/5
200/200 [==============================] - 61s 305ms/step - loss: 0.0357 - acc:
0.9950 - val_loss: 0.0338 - val_acc: 0.9950
Epoch 4/5
200/200 [==============================] - 61s 305ms/step - loss: 0.0343 - acc:
0.9950 - val_loss: 0.0334 - val_acc: 0.9950
Epoch 5/5
200/200 [==============================] - 61s 304ms/step - loss: 0.0340 - acc:
0.9950 - val_loss: 0.0330 - val_acc: 0.9950
Saved model to disk
root@e198f6ccc9aa:/home/dgxuser120/data#
```

Figure 7. Model Summary

The Figures 5, 6, 7 represents the layers and output shape of the each layer with the trainable parameters and number of classes with accuracy metric.

5.4 Parameters Evaluation

The model generates 99.50% accuracy and 99.5% model accuracy on identifying the handwritten signatures .The loss and val_loss parameters error rate is 0.0340 and 0.030. The model starts the 99 percent accuracy at the step of epoch 5. Figure 8 shows the comparison of the accuracy and model accuracy, loss and model_loss.

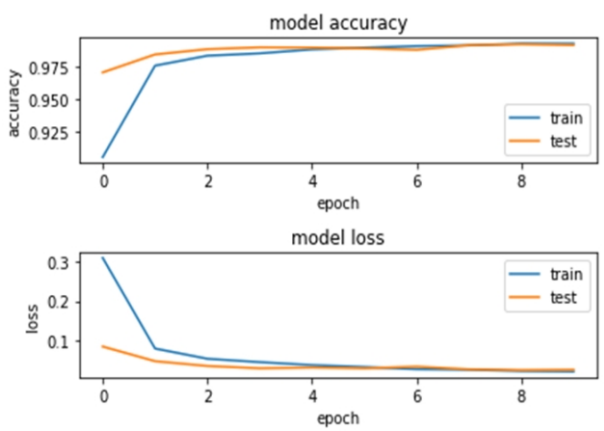

Figure 8. Comparison of Accuracy and Model Accuracy, Loss and Model Loss

6. Analysis of the Security Protocol using Scyther

The protocol analyzer Scyther (CISPA, n.d) is used for validation of the proposed methodology. It is configured to initiate various types of attacks. The scheme is analyzed for 1000 runs where both the user and BS run the scheme to exchange the required messages. During the execution, Scyther launched different types of attacks with the assumption of attacker has the initial knowledge of the system. The vulnerability of scheme is based on the parameters h(userID), h(password), and handwritten signatures. If these credentials are ignored at any stage then the entire scheme is futile. The strength of these parameters as evaluated by Scyther identified that in the absence of security these parameters are falsified and Man-in-the-Middle attack can be launched. Table 2 provides the detailed security analysis of the claims that are validated using Scyther.

The analysis of our security protocol based on Scyther validation indicates the proposed scheme supports against all of the claims that are proposed in the scheme.

Claim 1: UID remains unrevealed throughout the

S.No	Claim	Status	Attack
1	h(userID)	OK	No Attack initiated
2	h(password)	OK	No Attack initiated
3	Handwritten signature	OK	No Attack initiated
4	Aliveness	OK	No Attack initiated

Table 1. Parameters Checking using Scyther

registration and authentication process.

UID is an important parameter that will be useful for identifying the identity of the user. The anonymity of the user is supported in this scheme by converting user ID into hash (UID).

Claim 2: Password is secret.

The password security is based on the user in terms of user cannot revealed to anyone. The strength and security of the password claim is validated by Scyther.

Claim 3: Handwritten Signatures of the user is secret and features extraction is effective.

The hand written signatures of the users are stored in the private cloud and the effective feature extraction is performed using DeepCNN model. The claim that handwritten signature is secret is verified using Scyther.

Claim 4: CU and the BS, and CAS remains alive during the protocol execution.

The user, bank server, and cloud authentication server is said to be alive.

The above mentioned claims are validated by evaluating the strength and security based on multiple runs. The main concept included in the proposed scheme is hashing and effective feature extraction. The adoptability of the private cloud for storing the bank and the user credentials makes the proposed scheme secure, and provides a means for integrity check. Even if any attacker observes the message that is transmitted during the registration and authentication process, it is not possible for the attacker to interpret the accurate handwritten signature.

6.1 Effectiveness of Proposed Authentication Protocol

The proposed scheme is compared with the traditional password based authentication mechanisms and biometric authentication mechanisms. The traditional password based mechanisms computationally effective but the recent cyber attacks on the cloud shows the need of the strong multi factor authentication (Philip, & Bharadi, 2016). To develop the authentication of the user using handwritten signatures is more practical way for the banking industry. The employees of banking sector uses signature of the user to cancel or maintain the accounts, transactions, and check identification manually. The same concept adopts for the authentication of the bank users in the cloud environment. Philip et al. (Bommagani, Valenti, & Ross, 2014) Signature verification scheme, a SaaS implementation on Microsoft Azure Cloud using the Webber Local Descriptor and classification using K-nearest Neighborhood achieved 92.50% performance index and 94.25% correct classification rate. Offline signature recognition and verification scheme using back propagation and Neural fuzzy techniques are proposed in (Choudhary, Patil, Bhadade, & Chaudhari, 2013; Mehra, & Gangwar, 2014).

6.2 Comparison with Existing Methods

The DeepCNN model is adopted in our proposed framework to recognize and verifying the handwritten signatures. The DeepCNN model has more than one hidden layer to extract the features effectively. The model accuracy is based on the parameters defined in the layers and the model is suitable for large data set. The user credentials and handwritten signatures are stored at the private cloud which is more securable and configurable compare to the public cloud. The authentication server of the cloud verifies the credentials of the user without storing the credentials at the public cloud. By comparing with the existing schemes (Nagaraju, & Parthiban, 2015; Dey, Sampalli, & Ye, 2016; Prasanalakshmi, & Kannammal, 2012) the proposed scheme have the following advantages and the comparison details are represented in the Table 3:

- There is no need of storing credentials at the public cloud.
- Privacy of the credentials is preserved at the private cloud.
- There is no storage limitation as the proposed scheme adopts cloud storage.
- The feature extraction of the handwritten signatures is

Methods	Privacy Preservation of the Credentials	Traditional Authentication	Biometric Authentication	Variation of the Biometric Factor	Feature Extraction
Nagaraju et al. [31] Method	Yes	Yes	Yes	Yes	Not Specified
Dey et al. [41] Method	Yes	Yes	No	-	-
PrasanthiLakshmi et al. [42] Method	Yes	Yes	Yes	Yes	Not Specified
Proposed Method	Yes	Yes	Yes	No	Specified

Table 2. Comparison with the Existing Methods

performed using DeepCNN model with the dense activation function.

- Handwritten signatures are unique and can't be changed based on the age factor.

Conclusion

Adoption of cloud in the bank organization is a challenging task due to security and privacy concerns. In this paper, we proposed a new authentication mechanism using hand written signatures as a third factor and the extraction of the signature features are effectively performed using DeepCNN model. The adoption of the CNN model in the cloud improves the 99% accuracy of the proposed authentication scheme. Experimental results shows the accuracy of the model which is based on the defined hyper parameters. The scheme is simulated under NVIDIA GPU system using Python Keras API. GDPS handwritten signatures are used in the proposed scheme with 200 classes of the 200 users signatures with 10800 images belonging to 200 classes.

References

[1]. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. https://doi.org/10.6028/NIST.SP.800-145

[2]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R.,.....& Zaharia, M. (2010). *A view of Cloud Computing, Communications of the ACM* https://doi.org/10.1145/1721654.1721672

[3]. Suresh, M. C. (2010). Cloud computing: strategic considerations for banking & financial services institutions. *TCS White Papers,* 1-24.

[4]. Yan, G. (2017, July). Application of Cloud Computing in Banking: Advantages and Challenges. In *2017 2nd International Conference on Politics,* Economics and Law (ICPEL 2017). Atlantis Press. https://doi.org/10.2991/icpel-17.2017.8

[5]. Carroll, M., Van Der Merwe, A., & Kotze, P. (2011, August). Secure cloud computing: Benefits, risks and controls. In *2011 Information Security for South Africa* (pp. 1-9). IEEE. https://doi.org/10.1109/ISSA.2011.6027519

[6]. Hamidi, N. A., Rahimi, G. M., Nafarieh, A., Hamidi, A., & Robertson, B. (2013). Personalized security approaches in e-banking employing flask architecture over cloud environment. *Procedia Computer Science,* 21, 18-24. https://doi.org/10.1016/j.procs.2013.09.005

[7]. Huang, C. Y., Tzeng, W. C., Tzeng, G. H., & Yuan, M. C. (2011). Derivations of information technology strategies for enabling the cloud based banking service by a hybrid MADM framework. In *Intelligent Decision Technologies* (pp. 123-134). Springer, Berlin, Heidelberg. Retrieved from https://link.springer.com/chapter/10.1007/978-3-642-22194-1_13

[8]. Catteddu, D. (2009, December). Cloud Computing: benefits, risks and recommendations for information security. In *Iberic Web Application Security Conference* (pp. 17-17). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-16120-9_9

[9]. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems,* 28(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006

[10]. Rani, S., & Gangal, A. (2012). Security issues of banking adopting the application of cloud computing. *International Journal of Information Technology,* 5(2), 243-246.

[11]. Adjei, J. K. (2015). *Explaining the Role of Trust in Cloud Computing Services.* Info, 17(1), 54-67. https://doi.org/10.1108/info-09-2014-0042

[12]. Lee, S., Ong, I., Lim, H. T., & Lee, H. J. (2010). Two factor authentication for cloud computing. *Journal of Information and Communication Convergence Engineering,* 8(4), 427-432. https://doi.org/10.6109/jicce.2010.8.4.427

[13]. Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011, December). A strong user authentication framework for cloud computing. In *2011 IEEE Asia-Pacific Services Computing Conference* (pp. 110-115). IEEE. https://doi.org/10.1109/APSCC.2011.14

[14]. Banyal, R. K., Jain, P., & Jain, V. K. (2013, September). Multi-factor authentication framework for cloud computing. In *2013 5th International Conference on Computational Intelligence,* Modelling and Simulation (pp. 105-110). IEEE. https://doi.org/10.1109/CIMSim.2013.25

[15]. Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing,* 72(10), 3826-3849. https://doi.org/10.1007/s11227-015-1610-xv

[16]. Liu, W., Uluagac, A. S., & Beyah, R. (2014, April). MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data. In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 518-523). IEEE. https://doi.org/10.1109/INFCOMW.2014.6849285

[17]. Trevathan, J., & McCabe, A. (2005). Remote handwritten signature authentication. In *ICETE* (pp. 335-339). Retrieved from https://scitepress.org/papers/2005/14192/14192.pdf

[18]. Lee, J. K., Ryu, S. R., & Yoo, K. Y. (2002). Fingerprint-based remote user authentication scheme using smart cards. *Electronics Letters,* 38(12), 554-555. https://doi.org/10.1049/el:20020380

[19]. Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2019). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimedia Tools and Applications,* 78(12), 16345-16361. https://doi.org/10.1007/s11042-018-7012-3

[20]. Hossain, M. S., & Muhammad, G. (2015). Cloud-assisted speech and face recognition framework for health monitoring. *Mobile Networks and Applications,* 20(3), 391-399. https://doi.org/10.1007/s11036-015-0586-3

[21]. Pang, S., Kim, D., & Bang, S. Y. (2003). Membership authentication in the dynamic group by face classification using SVM ensemble. *Pattern Recognition Letters,* 24(1-3), 215-225. https://doi.org/10.1016/S0167-8655(02)00213-1

[22]. Kumar, C. R., & Bindu, A. (2006, November). An efficient skin illumination compensation model for efficient face detection. In *IECON 2006-32nd Annual Conference on IEEE Industrial Electronics* (pp. 3444-3449). IEEE. https://doi.org/10.1109/IECON.2006.348133

[23]. Sun, Y., Wang, X., & Tang, X. (2014). Deep learning face representation from predicting 10,000 classes. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 1891-1898). Retrieved from http://mmlab.ie.cuhk.edu.hk/pdf/YiSun_CVPR14.pdf

[24]. Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., ... & Adam, H. (2017). *Mobilenets: Efficient Convolutional Neural Networks for Mobile Vision Applications.* arXiv preprint arXiv:1704.04861. Retrieved from https://arxiv.org/pdf/1704.04861.pdf

[25]. Hu, J., & Chen, Y. (2013, August). Offline signature verification using real adaboost classifier combination of pseudo-dynamic features. In *2013 12th International Conference on Document Analysis and Recognition* (pp. 1345-1349). IEEE. https://doi.org/10.1109/ICDAR.2013.272

[26]. Rivard, D., Granger, E., & Sabourin, R. (2013). Multi-feature extraction and selection in writer-independent off-line signature verification. *International Journal on Document Analysis and Recognition (IJDAR),* 16(1), 83-103. https://doi.org/10.1007/s10032-011-0180-6

[27]. Eskander, G. S., Sabourin, R., & Granger, E. (2013). Hybrid writer-independent–writer-dependent offline signature verification system. *IET Biometrics,* 2(4), 169-181. https://doi.org/10.1049/iet-bmt.2013.0024

[28]. Bertolini, D., Oliveira, L. S., Justino, E., & Sabourin, R.

(2010). Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. *Pattern Recognition,* 43(1), 387-396. https://doi.org/10.1016/j.patcog.2009.05.009

[29]. Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognition,* 70, 163-176. https://doi.org/10.1016/j.patcog.2017.05.012

[30]. Sun, Y., Chen, Y., Wang, X., & Tang, X. (2014). Deep learning face representation by joint identification-verification. In *Advances in Neural Information Processing Systems* (pp. 1988-1996). Retrieved from http://www.ee.cuhk.edu.hk/~xgwang/papers/sunCWTnips14.pdf

[31]. Nagaraju, S., & Parthiban, L. (2015). Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. *Journal of Cloud Computing,* 4(1), 22. https://doi.org/10.1186/s13677-015-0046-4

[32]. Montserrat, D. M., Lin, Q., Allebach, J., & Delp, E. J. (2017). Training object detection and recognition CNN models using data augmentation. *Electronic Imaging,* 2017(10), 27-36. https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-163

[33]. Kuo, C. C. J. (2017). The CNN as a guided multilayer recos transform [lecture notes]. *IEEE Signal Processing Magazine,* 34(3), 81-89. https://doi.org/10.1109/MSP.2017.2671158

[34]. Strom, N. (2015). Scalable distributed DNN training using commodity GPU cloud computing. In *Sixteenth Annual Conference of the International Speech Communication Association.* Retrieved from https://www.isca-speech.org/archive/interspeech_2015/i15_1488.html

[35]. Goud, N.(n.d). *Cyber Attack on Cloud Computing Company makes France News Websites go Dark.* Retrieved from https://www.cybersecurity-insiders.com/cyber-attack-on-cloud-computing-company-makes-france-news-websites-go-dark/

[36]. Philip, J., & Bharadi, V. A. (2016). Signature Verification SaaS Implementation on Microsoft Azure Cloud. *Procedia Computer Science,* 79, 410-418. https://doi.org/10.1016/j.procs.2016.03.053

[37]. Bommagani, A. S., Valenti, M. C., & Ross, A. (2014, October). A framework for secure cloud-empowered mobile biometrics. In *2014 IEEE Military Communications Conference* (pp. 255-261). IEEE. https://doi.org/10.1109/MILCOM.2014.47

[38]. CISPA (n.d). Cas Cremers, *Instructions, Helmholtz Center for Information Security.* Retrieved from https://people.cispa.io/cas.cremers/scyther/install-generic.html

[39]. Choudhary, N. Y., Patil, M. R., Bhadade, U., & Chaudhari, B. M. (2013). Signature Recognition & Verification System Using Back Propagation Neural Network. *International Jorunal of IT,* Engineering and Applied Sciences Research (IJIEASR), 2(1), 1-8. Retrieved from https://pdfs.semanticscholar.org/b8b3/4e31deac1bab5ea2291a186dedcbb9500179.pdf

[40]. Mehra, R., & Gangwar, D. R. (2014). Enhanced Offline Signature Recognition Using Neuro-Fuzzy and SURF Features Techniques. *International Journal of Computer Science and Information Technologies,* 5(5). Retrieved from https://pdfs.semanticscholar.org/09d6/28a889c944086ec52291348ddae2a6baa21d.pdf

[41]. Dey, S., Sampalli, S., & Ye, Q. (2016). MDA: message digest-based authentication for mobile cloud computing. *Journal of Cloud Computing,* 5(1), 18. Retrieved from https://link.springer.com/article/10.1186/s13677-016-0068-6

[42]. Prasanalakshmi, B., & Kannammal, A. (2012). Secure credential federation for hybrid cloud environment with SAML enabled multifactor authentication using biometrics. *International Journal of Computer Applications,* 53(18). Retrieved from https://pdfs.semanticscholar.org/cf2f/440296f9e213bf5aa81800778819bfbb132e.pdf

ABOUT THE AUTHORS

K. Devi Priya working has over 12 years of experience in the Department of Computer Science and Engineering at Aditya Engineering College, Surampalem, Andhra Pradesh, India and pursuing a Ph.D. from the Jawaharlal Nehru Technological University, Kakinada Andhra Pradesh, India. Her research area includes Cloud computing, Cyber Security, Deep learning, and Big Data Anlaytics. She is the member of the Leadingindia.ai AI & Deep Learning research.

Dr. L.Sumalatha has over 19 years of teaching experience in Computer Science & Engineering Department at University College of Engineering Kakinada. Her areas of interest are NLP, Machine Learning & Cloud and Cyber Security. Currently she is the Director for Industry Institute Interaction Placements & Skill Development, Jawaharlal Nehru Technological University, Kakinada Andhra Pradesh, India. She is the Research Lead of AI Platoon research group with leadingindia. ai- AI & Deep Learning research initiative. She has about 35 research publications.