A Study of Security Mechanism using Face Detection, Attribute Based Encryption (ABE) and Deep Learning in field of Cloud and IoT.

Sampath Yelchuri [1]

[1] *Graduate Student, Department of Computer Science*, Bowling Green State University, Ohio, USA

Abstract - **This paper mainly focuses on data security in the field of cloud and IoT. In today's world, usage of cloud and IoT has become more generic. Nowadays, many applications use cloud and IoT as key elements to offer various services. As there is a tremendous growth in the usage of IoT devices, huge amount of data is being generated and this data is being stored in a virtual data center known as cloud. There are many users who access cloud and there is a necessity to provide security for the data. Since we have mechanisms which work only on encryption and decryption of the data, it is also necessary that there must be an approach or scheme which can maintain both authenticity and security for user(s) data. For this, we have proposed an experimental study which uses two emerging technologies i.e., Deep Learning and Attribute Based Encryption (ABE) to enhance security. This research also gives an overview on user(s) authenticity and security for the data using Face Detection, Attribute Based Encryption (ABE) and Convolutional Neural Networks (Covnets). We examine this approach by conducting an experiment which gives a future scope of integrates FDS with ABE and Deep Learning techniques.**

Keywords— Cloud, Internet of Things (IoT), Attribute Based Encryption (ABE) and Convolutional neural networks (Covnets).

I. INTRODUCTION

Nowadays, distributed systems like Cloud Computing and Internet of Things (IoT) have brought tremendous changes in the world. The term "Cloud Computing" is defined as a virtual system which offers an easy ad-hoc network access to a shared pool computing resources [1]. A cloud computing service offers its user(s) or client(s) an efficient data servers which provide software, hardware and information resources. User(s) or client(s) interact with the cloud and use resources offered by it on a pay per user basis [2]. Cloud computing works on the basis of three service models. These are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). With the help IaaS, cloud users can get infrastructure components like processing power and storage space for storing the data. The PaaS gives the cloud users a temporary space or a run time environment to design and deploy their applications. Using the SaaS service model, users are in a position to readily use the applications which are already deployed into the cloud. The expression "Internet of Things (IoT)" is fundamentally regarded as a small computing device which has the capability to hold small amount of memory and processing power. Additionally, the IoT devices have various issues with respect to quality, execution and security. Since IoT devices has less storage capacity and computation power, cloud computing offers storage through a shared pool of resources which can be dynamically allocated and can easily be obtained by an IoT device [3].

The IoT devices are capable of producing huge amount of data which can be stored and processed in the cloud. So, it is very important to keep the data private and safe. One of the key difficulties in Internet of Things (IoT) and Cloud computing is data security. Dependability, economy, efficiency and viability of the security and protection are fundamental factors for guaranteeing secrecy, honesty, validation and access control in Cloud and IoT.

There are few mechanisms in IoT and cloud regarding security and protection of the data. The most traditional scheme is the Homomorphic Encryption in which a stranger or an unauthorized entity has the scope of manipulating the encrypted text without the password or secret key [4]. Another current technique which is used for maintaining privacy of the data is authentication using Face Detection System (FDS). Using this method users willing to access data on the cloud are required to be authenticated prior using FDS [5]. To enhance data security mechanisms in multi-cloud communication in IoT, Attribute Based Encryption (ABE) is utilized. So, our main objective in this research is to study how deep learning technology can be used to provide security for the data that is being transmitted between cloud and IoT devices.

Here we propose a new approach for enhancing more security using Face Detection System (FDS), deep learning mechanism with Attribute Based Encryption (ABE). The remaining paper is organized as follows: initially in Section I we discuss some of the related works which are currently being used for encrypting and decrypting the data on the cloud and face recognition system. In Section III, we discuss about the approach for this research followed by Section IV where we discuss about our experiment and its result which is conducted by taking a set of 20 images of five users in different positions. In Section V, we discuss about the threats to validity and Section VI, we conclude this paper by showing the future scope of the research.

II. RELATED WORK

Some of the existing methodologies which are already proposed are given below:

Thirumalai et al. [6] discussed the Memory Efficient MultiKey (MEMK) generation scheme. For very sensitive data, this method will help in transferring data from Cloud to IoT and IoT to Cloud. It is very important to create public and private keys while encrypting the data. For memory efficiency, this scheme reuses the RSA scheme with a Diophantine form of the nonlinear equation. Because of the reason that this scheme uses only the RSA public key, it produces efficient results in encrypting the data.

Huang et al. [7] presented a safe, proficient and fine-grained information control structure which uses the Hierarchical ABE (HABE) for IoT. In this method, decryption is only done when the attributes of the IoT devices are matching with the access policies. Here, for updating the access policy the IoT device produces an update key which is outsourced to the cloud. Using this update key, the cloud server modifies the access policy which is required

to decrypt the cipher text. Although, this policy updating task is out sourced to the cloud, it does not reveal any kind of sensitive data to the server.

Alrawais et al. [8] in his writing, made an encoded key trade convention to build up secure transfer of data or information among a group of cloud and IoT devices. The key exchange convention used Digital Mark and Cipher text - Policy based ABE (CP-ABE) techniques to accomplish a few essential security objectives. CP-ABE gives an access structure to encode information, and requires only a subset of the characteristics for decoding. Since the secret key includes one kind of arbitrary number for each property in the entrance arrangement, CP-ABE ensure against conspiracy assaults.

Naveen et al. [9] have proposed a face detection and authenticity scheme which can extract the face of the user(s) using two methods. One is Local Binary Pattern (LBP) and the second is Binarized Statistical Image Features (BSIF) which is used for extracting the patterns in the user(s) face. This system has the ability to detect and check whether the user(s) has a facial cover or not which resembles the face of another user. This system has the ability to extract features and texture of the user(s) face from a two dimensional images and can classify whether it is a real face or a facial cover.

So, as we have many standalone security schemes which majorly focus on encrypting and decrypting the data. But we don't have any approach which maintains both the authenticity and security for the data in the cloud. With the integration of new technologies such as Face Detection System (FDS), Attribute Based Encryption (ABE) and Convolutional Neural Networks (Covnets), we can maintain the user(s) authenticity and security for the data in the cloud. So, here we provide a new approach which ensures both user(s) authenticity and data security using the trending technologies.

III. Approach

In this paper, we introduce a new approach which provides security for the data by checking the authenticity of user(s) with the help of Face Detection System (FDS) [4], Attribute Based Encryption (ABE) and a Deep Learning concept named Convolutional Neural Networks (Covnets) to enhance security in cloud and IoT.

Initially, user or client authentication plays an important role in maintaining security. So, here we are giving user(s) face as input for authorization. For this we design a system as shown in figure 1 called Face Detection System (FDS) which aims at capturing and extracting features from a face of a user who is trying to access the cloud. This FDS plays a crucial role in formulating a data structure which is known as the template to store all the features extracted from the user(s). For new user(s), we take the personal details of the user(s) like mobile number or email id for registering into the FDS.

Fig.1 User Authentication to Cloud using FDS [4]

FDS takes user(s) face as input and authenticates into the cloud.

These two things (i.e., features extracted from the user(s) face and mobile number or email id) are stored in a data server. Along with these features, this data server also stores the mean and standard deviation of each feature of the image that is captured by the FDS for classification of different similar images into set of classes. Using these features as key attributes, we encrypt the data of user(s) with the help of Attribute Based Encryption (ABE) scheme.

Now, with the help of the template generated by FDS, we give this as input to the Convolutional Neural Network (Covnets). This Covnets helps in forming layers of attributes by classifying all the features that are gathered in the FDS template. Here we use three layers for the classification of the features. The first layer includes features like lines, edges and curves. The second layer stores the shapes like nose, mouth, eyes and ears which are directly taken from image. And the final layer stores the whole face pattern of the user.

Here we use the FDS which was proposed by *Pawar V. P* [4] to detect the face and features of a user or client. The process of extracting face from an input image is carried out by following the below steps as shown in figure 2:

Step 1: The first and foremost thing is to capture the image of the user or client. This can be done by embedding an IoT device in the FDS system which is capable of capturing pictures with good resolution.

Step 2: In this step, the system has to detect only the face as a major element in the entire captured image. In other words, from the whole image that has been captured by the system, the Face Detection System (FDS) has to separate the face from other un-necessary objects.

Step 3: Now, in this step the system has to mainly focus on the facial structure of the image and has to grasp some attributes or properties that form a unique pattern.

Step 4: Finally, all the properties which have been extracted in the previous step are organized in a systematic way and are stored in a database which will helpful in encoding the data.

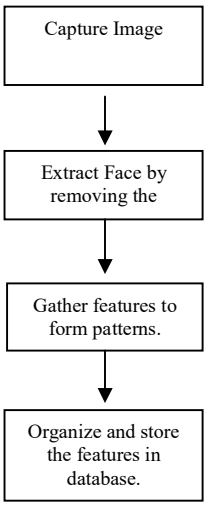

Fig.2 Flow diagram of features extraction [4]

Different phases in FDS for extracting features from the image captured.

Once these features are systematically stored in a data base, we can use them for encrypting the data. Giving these

features as input to the Attribute Based Encryption (ABE) scheme as shown in fig. 3, encoding of the data is done. This process of encryption is more effective as the features extracted from the FDS stands unique from person to person.

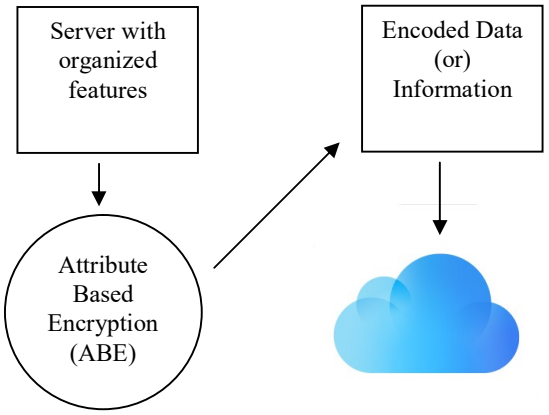

Fig. 3 Encryption of the data and sending to cloud [4]
Encrypting user data with the help of ABE by giving user face features as input from the server.

Now as shown in figure 4, the data of the client or user is encrypted using ABE scheme and is stored in the cloud. Later, if any user wants to access this encrypted data they have to initially give the face as the input for the authentication. Now the FDS takes the user face as the input and checks with the features that are previously stored in the data base. The FDS provides authentication by comparing the mean value of the features of newly captured image with the existing image feature mean value. Here we consider a confidence interval value from 0 to 3.Since it is impossible to build a system with 100% accuracy, we are using this confidence interval to maintain 97% accuracy for the FDS system. If the difference between the two means values lies in between 0 and 3, then the client or user is given the authorization to access the data on the cloud.

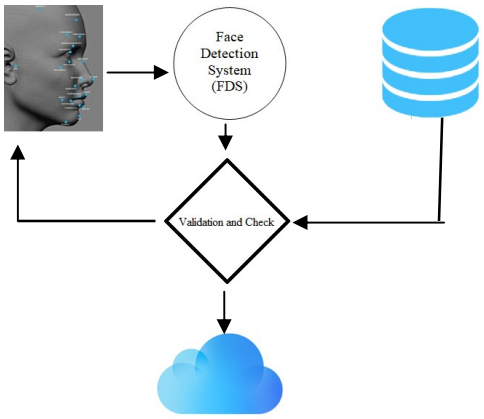

Fig. 4 Entire System Design [4]
FDS take user face as input and calculates the difference of feature mean value by accessing the server and authenticates the user into cloud.

With this approach it is possible to maintain both authentication and high security for the user(s) data. The figure 5 represents the flow diagram of the entire approach which is used for authentication and data security.

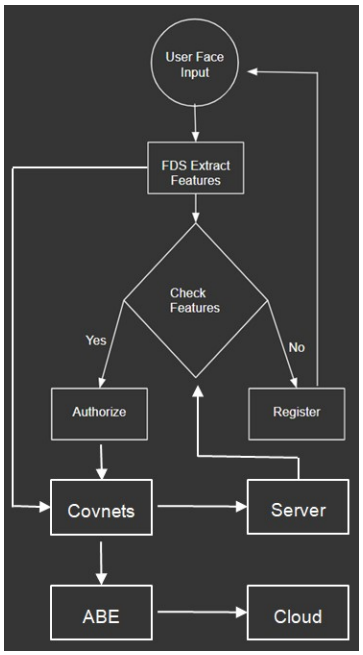

Fig. 5 Integrating FDS with ABE and Covnets [4]
User(s) gives his face as input and the FDS extracts the features from the image captured. The FDS checks the face feature mean value in the server and calculate the difference between the extracted and stored values and if this value is less than 3, the user is given authorization. Using the features classified using Covnets, we encrypt the data using ABE scheme and store the user data in the cloud.

We have also considered a case study where a new user who wants to store the data in the cloud. Now, we make use of user's personal data like Mobile Number and Email Id for registering the user. Along with this data, we also capture the face of the user using a camera and send the images as input to the FDS. The FDS sends this captures image to the Covnets component which classifies and extracts the features from the image and also calculate the mean and standard deviation of all the features collected and classify all the similar features into a single class for that particular user.

Even though, if the user gives a face image in an inclined angle, the features of user remains similar but not exactly the same. So all these similar features are sorted and then classified into one class for that particular user. This class is used as the identification class of the user which is used as the key aspect for authenticity.

Now the user is allowed to store the data or information in the cloud by encrypting the data using Attribute Based Encryption (ABE). The Attribute Based Encryption (ABE) uses the features of user which are extracted by the FDS for encoding the data.

Every time a user gives the face as input to the FDS, it treats every face as a new face and checks the features extracted from the FDS and checks with the template which is generated by Covnets which is stored in the Server including the mean and standard deviation. Now, checking is done in the FDS by calculating the difference between the original mean value of the face feature of the data owner and the mean value which is newly calculated for the user who is trying to access the data on cloud. If the difference between the two feature mean values is less than 3, then the user is matched with any one class among various set of image classes which are formed by providing a training data set which is discussed in the Experiment and Results section.

By this approach, we can provide both authentication and security for the data which is stored in cloud using FDS, ABE and Convolutional Neural Networks.

IV. Exteriment and Results

Initially, we have considered a set of 16 images of four different persons. These 16 images are classified into four classes like class-1, class-2, class-3 and class-4 as shown in figure 6. Each class is dedicated for a single person which is a collection of images of that person taken at different angles.

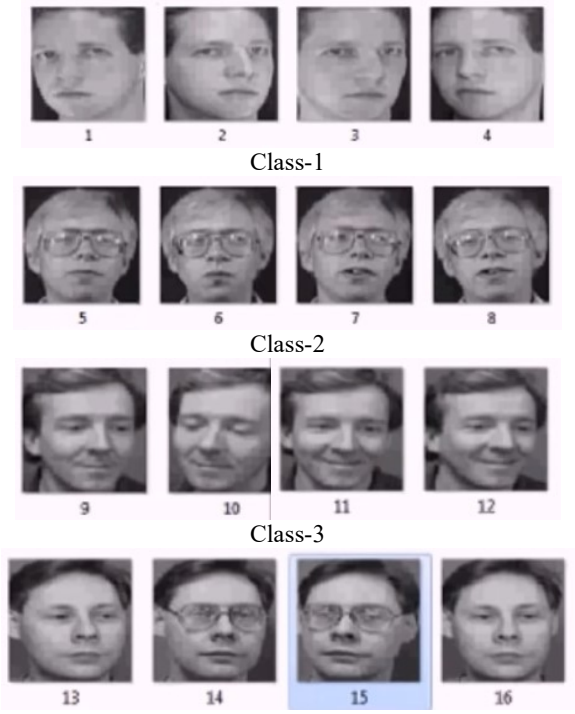

Fig. 6 Classes of Images of four different persons [10].
16 images of four persons are taken at different angles and classified into four classes like Class-1, Class-2, Class-3 and Class-4.

Now, have selected four images out of all the 16 images in such a way that each these four images include an image from each class. Now these four images are given as input to the FDS system as a training data set where it calculates the mean feature value of each image and stores it into the server. The training output includes three values whenever an image is given as an input to the FDS system. The two values are labeled as Mean Feature Value, Standard Deviation and Class of the Image. The Mean and Standard deviation values of the face features are calculated by measuring length of the lines and curves which are extracted from the FDS system and stored in the first layer of Covnets. Since we have trained four images, the server contains four rows of data which is generated by the FDS system as shown in the figure 7.

	1	2	3
1	Mean of Feature	Standard Deviation	Class of Image
2	143.2204	12.7103	1
3	142.8456	10.6213	1
4	111.7982	9.8543	2
5	110.5772	9.5401	2

Fig. 7 Server stores the output from FDS.
Output values generated and stored in a server when the four images are given as input to train the FDS system.

Now, with the help of this trained data which is stored in the server, we chose another image from a class and gave it as an input as a test data to the FDS system as shown in figure 8 and checked whether the FDS system was able to project which class does the image belong to. The FDS system calculated the mean feature value of this test data and compared the difference with all the existing mean feature values. Once the difference is calculated, it selects the minimum value out of all the difference values and fetches the class value from the server. And the results were quite interesting.

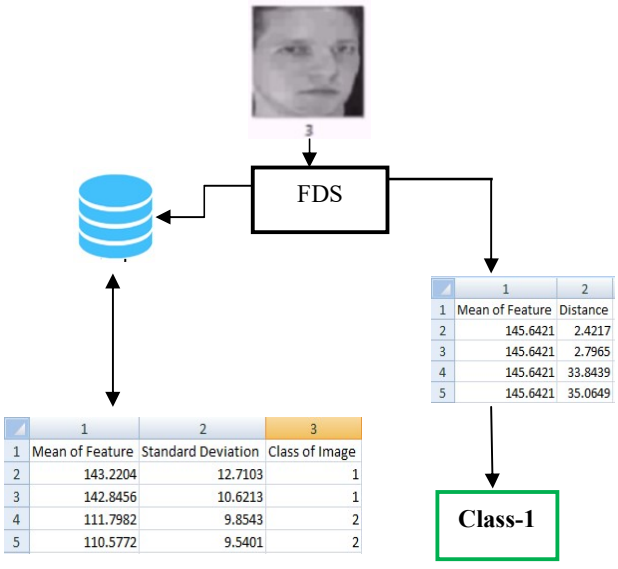

Fig.8 FDS checks which class does image belong to.
The FDS system calculates the difference of mean feature value using the values stored in sever and projects the class as output.

Now the image was classified as class-1 and the user was given an authorization into the cloud and was able store data in cloud by encrypting the information with the help of

Attribute Based Encryption (ABE) which uses the features which were newly extracted from the test image.

For encrypting the data, we have used the newly extracted features of the FDS instead of the existing features. Using these features as private key we have encrypted the user data and stored the information in the cloud.

V. THREATS TO VALIDITY

The following are the threats or system failures that may occur in the FDS system:

- There might be few cases when the IoT device which is capturing the user or client face for authentication may not completely extract the features of the face.
- As in the above case, if the features of the face are not being extracted then it may sometimes result in such a case it would be difficult to encrypt the data using ABE.
- As we are using the mean values to represent the features of an image captured and storing these values in a server, there is a possibility that the FDS generated same feature mean value for set of images due to the similarities. So when we calculate the difference between the actual and the stored value the classification of the person into a class becomes difficult.
- So, the above issue sometimes make the FDS does not authorize the user since he/she might not fall into any of the class of persons who are authorized.

VI. CONCLUSION

With the modern technology, we can improve the level of security using FDS, Attribute Based Encryption and Deep Learning mechanism. Here in this case, this is just a study or approach on how to integrate the new things. But, moving forward we can practically implement this model to maintain the authenticity and privacy for the data stored in the cloud and IoT. There is a huge scope for ABE and Deep Learning mechanisms where systems can be built and learn themselves to enhance more security.

Coming down the line, we would work more Covnets that helps the FDS system to learn and predict the face of the user more efficiently. And moreover, we would also concentrate on how to overcome some the threats that were mentioned in the above section.

REFERENCES

[1] "National Institute of Standards and Technology," NIST, 30-Nov-2018. [Online]. Available: https://www.nist.gov/. [Accessed: 03-Dec-2018].

[2] Rajaraman, V. (2014). "Cloud computing. Resonance", 19(3), 242-258. doi:10.1007/S12045-014-0030-1.

[3] Liu, Y., Dong, B., Guo, B., Yang, J., "Combination of cloud computing and net of things (IOT) in medical observance systems", International Journal of Hybrid info Technology, 2015.

[4] Yang, Xue and Fan Yin. "A Fine-Grained and Privacy-Preserving question theme for Fog Computing-Enhanced Location-Based Service.", Sensors 17.7 2017.

[5] A. A. Pawle and V. P. Pawar, "Face recognition system (FRS) on cloud computing for user authentication," vol. 3, no. 4, 2013.

[6] C. Thirumalai and H. Kar, "Memory efficient multi key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices," 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 2017.

[7] Huang, Qinlong, Licheng Wang, and Yixian rule. "DECENT: Secure and fine-grained information access management with policy change for affected IoT devices." World Wide net 2017.

[8] Alrawais, A., Alhothaily, A., Hu and C., Xing, X. "An Attribute-Based cryptography theme to Secure Fog Communications". IEEE Access, 2017.

[9] S. Naveen, R. S. Fathima, and R. S. Moni, "Face recognition and authentication using LBP and BSIF mask detection and elimination," 2016 International Conference on Communication Systems and Networks (ComNet), 2016.

[10] Qiu, Meikang, Keke Gai, Bhavani Thuraisingham, Lixin Tao, and Hui Zhao. "Proactive user-centric secure information theme exploitation attribute-based linguistics access controls for mobile clouds in monetarybusiness." Future Generation laptop Systems , 2018.

[11] M. U. Rahman, "A comparative study on face recognition techniques and neural network," Computer Vision and Pattern Recognition, pp. 1–8, Oct. 2012.