Securing Cloud in Industrial IoT using Iris and Retina Scanner

S. Kalaiarasi, Srinidhi Sathyamurthy, Tanisha Garg, Pallavi Gupta

Abstract: Cloud computing has become extremely popular. It is one of the fastest evolving technologies. It is mostly used in industrial IoT, where the data generated is huge. It has many advantages. But there are also a few security issues we have to deal with when it comes to using the cloud. Data plays a very significant role in cloud computing. But data breaching can collapse a business. Also, any third party can log in to these cloud servers and use the valuable data for various other purposes. So trustworthy security measures have to be taken, to make sure that the information is protected and misuse of data does not take place. A few biometric methods have been implemented, but it not very cost-effective. And since the data is stored on remote servers, the data can never be a hundred percent safe. A new system has to be implemented, which is both easy to execute and demands less cost. This paper discusses how Iris and Retina scanners can be put together to ensure the security of the data stored in the cloud servers.

Keywords: IDS, Intrusion Detection, KDD-99, XGBoost.

I. INTRODUCTION

In cloud computing, we avoid using a personal computer or a local server. Instead, we use a network of remote servers that are hosted on the internet. Storing, managing and processing of data are done on these servers. We often go with this because the storage space offered by the cloud providers is unlimited. Suppose at first, the amount of data present in the database may be less. So, we can choose a plan offered by the cloud provider which offers a small amount of storage. Later, when the datasets present in the database grows with respect to time and size, we can upgrade to a different plan, taking into consideration the amount of data already available in the database and the growth of data in the upcoming days or months. So, expanding of storage is easily possible. Also, if the situation is vice-versa, that is, first we have a large set of data with lots of rows and columns and then the data shrinks with time then we can easily opt for a different plan which provides less storage space. It is usually done to reduce the wastage of storage space. Since so much data is stored by so many people in the cloud, securing the data becomes very important for both businesses as well as individual users. This is because all the clients want their data to be maintained securely. And that every business has legal obligations to keep the data safe. Therefore, security becomes an essential element when it comes to the cloud. Each person should check whether the correct security measures are being offered by the cloud providers before actually opting for it. Cloud antivirus and cloud backup are mostly used as a security plan. Cloud backup is used to ensure that if the worse happens data loss occurs due to any reason, then it can be restored to the latest backup. This is done very quickly. A few cloud security methods are Authentication and Identity, Data Encryption, Information integrity, and Privacy and Flooding Attack Solution.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author
Srinidhi Sathyamurthy*,Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. Email: srinidhi_sathyamurthy@srmuniv.edu.in
Tanisha Garg Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. Email: tanisha_garg17@srmuniv.edu.in
Pallavi Gupta Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. Email: pallavi_gupta17@srmuniv.edu.in

II. EXISTING SYSTEM

The Cloud used by Industries, let it be a private cloud or public cloud, user-authentication is done in a traditional way i.e. password. Some new developments like authentication using biometrics, which includes fingerprints, face recognition, signatures, tooth, etc. are also being used. We need to increase security because that will minimize the chances of false results. Since security becomes our major concern, we can proceed towards other highly secure authentication methods. Iris scans have been implemented in a few places. But Retina scans are only used in the fields of medicine, ATM identity verification, and government agencies like FBI, CIA and NASA. But the cost-effective system does not exist. Nor does an algorithm that can combine both iris and retina scans, to increase the effectiveness.

III. PROPOSED SYSTEM

The existing system claims to secure the cloud network which comprises a large number of datasets that are stored from Industrial IoT. There is a disadvantage of using fingerprints. Fingerprints can be replicated easily. Even signatures can be copied. Deformation can occur non-elastically as pupil changes size in the Iris scan. So, relying on iris alone will not provide to be so effective. During such a situation, we can combine both Iris and Retinal Scans. They are highly dependable as no two individuals can have the patterns. This way, the security of the cloud can be enhanced tremendously.

IV. IRIS AND RETINA SCAN

A. Iris Scan

The existing Iris Scan algorithm follows the following procedure:

The input image is first taken. Then it is transformed into Greyscale. Once it is converted into greyscale, it follows the process of Fast Fourier Transform.

The FFT decomposes an image into two major components: the real component and the imaginary component. The image in the frequency domain is represented in this layout. The input signal is in the frequency domain if the input signal is an image. The number of frequencies is equivalent to the spatial domain or number of pixels in the picture.

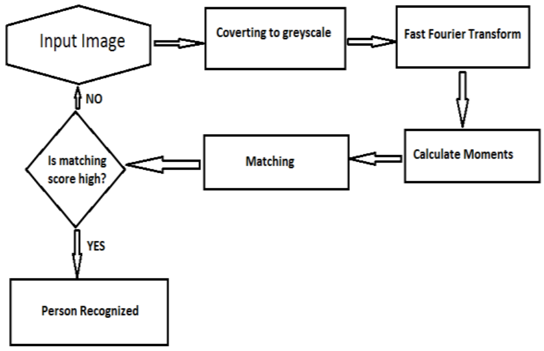

Fig. 1 Flowchart of Iris Scan Algorithm

FFT can be used as an alternative to linear spatial filtering. It is more proficient to use the Fourier transform in case of a large filter. It primarily permits us to detach and deal with dissimilar image frequencies. So low-pass filtering takes place with a higher degree of precision. After this, "Moments" are calculated. A string of numerical values are calculated, called moments. They recognize the shape of the object, such as area, centroid, the moment of inertia, orientation, etc. Let an image f(a,b) be taken as an object and the grey level of a pixel is believed to be the mass at a point of the object. For an image of size L*L, the (i,j)th moment of the image f(a,b) is defined as :

M(i,j)= ∑a ∑b ai bj f(a,b)

Now M(0,0)= ∑a∑b a0 b0 f(a,b) = ∑a ∑b f(a,b)

For matching the result with the input image, the Euclidean distance formula is applied. The 10 inputs are recognized. The eye images are obtained from the CASIA database. The algorithm is executed in the MATLAB platform. All the 10 final images are identified, and the recognition rate is roughly 100%.

1. Firstly, input the image of the eye.
2. The MATLAB code converts the image to grayscale.
3. The FFT point sequences concerning the image are then computed by the code.
4. Use the FFT point sequence to determine the sets of the normalized moments.
5. Input all the additional images for creating the database.
6. Take an input for matching.
7. The match is found by Euclidean Distance Formula.
8. Repeat steps 6 and 7.

B. Retina Scan

The existing retina scan algorithm consists of the succeeding seven significant steps:

1. Optic nerve and the identification of macula
2. Identification of Vascular Network
3. Elimination of noise
4. Detection of Branch points
5. Vascular Network Matching
6. Grouping of Branch Points
7. Matching of Vascular network

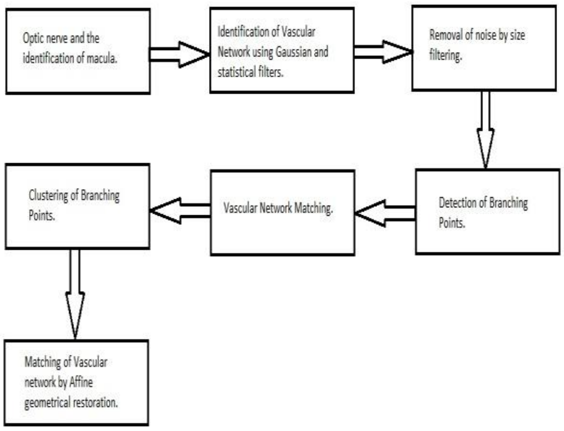
Optic nerve and the identification of macula.
Identification of Vascular Network using Gaussian and statistical filters.
Removal of noise by size filtering.
Detection of Branching Points.
Vascular Network Matching.
Clustering of Branching Points.
Matching of Vascular network by Affine geometrical restoration.

Fig. 2 Flowchart of Retina Scan Algorithm

This algorithm is based on the basic elements of a human eye i.e., optic nerve, macula and vascular network. The purpose of picking these three components is that the characteristics of these elements stay unaffected for a long time and degradations are likely to occur due to infections or illnesses. Before entering the processing states, the image of the retina is taken with the underlying requirements so that it can be utilized. The standards that should be fulfilled are the dimensions of the image, hue and the radiance standard. The required proportions are 512 x 512 pixels. For defeating the hindrance with images with poor intensity, its histogram is normalized. For accomplishing the agenda, the smallest intensity cost from each pixel in the picture is considered. Then all the pixels are divided by the greatest pixel intensity. The outcome obtained is a histogram that is stretched with increased difference.

1.Optic Nerve and Identification of Macula

The brightest section on the retina is the optic nerve disk. This scheme is based on a thresholding procedure. The center of mass is the midpoint of the optic nerve disk. The subsequent equation is taken:

$$x_i = \frac{\sum_1^m x_m}{m} \qquad y_i = \frac{\sum_1^n y_n}{n}$$

The distinguishing of the macula from the background has been the obstacle in most of the circumstances for macula detection. For mastering this problem, a region of interest – ROI is defined by the algorithm in which the macula recognition process is executed. Subsequently, for smoothening the intensity of the image, a Gaussian lowpass filter is used. The part which is set aside post filtering the input is the gray-level appearance in the plane parts. As the frequencies have been attenuated, the less sharp details have been left to the image. The equation below gives the thresholding value for the ROI:

$$thresh = \frac{mean(i) - std(i)}{2}$$

Here,

mean(i) : Statistical mean of the ROI
std(i): Standard deviation

Hough transformation is similarly acknowledged to be performed for the extremely precise optic nerve recognition as well as the macula detection methods.

2.Identification of Vascular Network

For the detection of the vascular network the algorithm is implementing a high pass Gaussian filter attenuating short frequencies while high refining.

The high pass Gaussian filter in two dimensions is given by,

$$H(u,\upsilon) = 1 - e^{-D^2(u,\upsilon)/2D_0^2}$$

Thresholding value is given by:

$$thresh = median(gs) - a \cdot std(gs)$$

Here,

median(gs): statistical median of the image
std: standard deviation
a: multiplier that is adjusted by the sample behaviour.

3.Elimination of noise

The algorithm executes numerous latest routines for eliminating the noise generated from the preceding steps of the algorithm. First, a framework of the segmented image is discovered and the delicate lines were described as objects and the size was decreased. For erasing the unwanted minute objects from the image, the process implements size thresholding. When the undesirable little objects are removed, the noise was detached using the mask filter outside the border of the retina. This mask is shaped by firm thresholding the primary image such that the non-zero values become white, neglecting only the important values behind.

4.Detection of Branch Points

The algorithm is performing a 2D convolution of a kernel. The pixels of vascular networks are used to determine branch points on the vascular network. Any pixel whose value is larger than 4 is regarded as a branch point. Small unnecessary prompts called parasitic elements are often presented in this procedure. The technique used for excluding these parasitic components is known as the pruning method. The outcome of this procedure is a matrix whose dimensions are equivalent to that of the initial image. The location of each non-zero pixel on the matrix denote a branch point on the original vascular network picture. Core of the identification algorithm is the intersections matrix of a retina.

5.Vascular Network Matching

$$\begin{bmatrix} x & y & 1 \end{bmatrix} = \begin{bmatrix} w & z & 1 \end{bmatrix} T = \begin{bmatrix} w & z & 1 \end{bmatrix} \cdot \begin{bmatrix} s\cdot\cos\theta & s\cdot\sin\theta & 0 \\ -s\cdot\sin\theta & s\cdot\cos\theta & 0 \\ \delta_x & \delta_y & 1 \end{bmatrix}$$

At this step of the algorithm, the chief identification process for the two given or abstracted retinal images takes place. The "distorted" intersections matrix will be geometrically manipulated. The optic nerve and its macula position match the position of the equivalent in the authentic matrix. Means for the execution of the above method is centered on the affine transform method. The transformation applied is linear conformal transformation, which protects angles and shapes. For this transformation, the matrix form is given as above, where,

w, z: coordinates of the image before the distortion
x, y: coordinates after the transformation
s: scaling factor
θ: rotational angle
δx, δy: variables of the translation.

6.Branch Points Clustering

The algorithm aims to remodel the deformed retina by intersecting it with the authentic image. The process acts wisely. It determines which of the branch points on must coincide.

The method is built on a straightforward prototype. A circular ROI is created at the distorted matrix. The center of the ROI has identical (a,b) coordinates.

7.Matching of Vascular network by Affine geometrical restoration

In this ultimate stage, the distorted intersections matrix is reconstructed by the algorithm that its branch points match with authentic points in the model. The way for gaining this outcome is by decreasing the mean space among the pairs in both matrices. Geometric affine transform is used.

$$\begin{bmatrix} x & y & 1 \end{bmatrix} = \begin{bmatrix} w & z & 1 \end{bmatrix} T = \begin{bmatrix} w & z & 1 \end{bmatrix} \cdot \begin{bmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ t_{31} & t_{32} & 1 \end{bmatrix}$$

The procedure attempts to recover the base points matrix by increasing the input points with the affine matrix. The most advanced square method techniques are employed for computing the parameters of the affine matrix.

V. PROPOSED ALGORITHM

For the scanning method to be successful, we need a database to store all the images and data associated with it so that the retina and iris images can be verified efficiently, just like the CASIA database. Fusing Iris and Retina scanning is an immense challenge because of the rich apparatus but it can be a huge success in the terms of security in IoT and other domains.

Algorithm:

1. Input the image of iris and retina.
2. The image processing of both iris and retina is done simultaneously but as different modules.
3. The existing system algorithm is used to verify iris and retina but it is programmed in such a way that the processing is done simultaneously and the input image is then checked with the database where the data is stored.

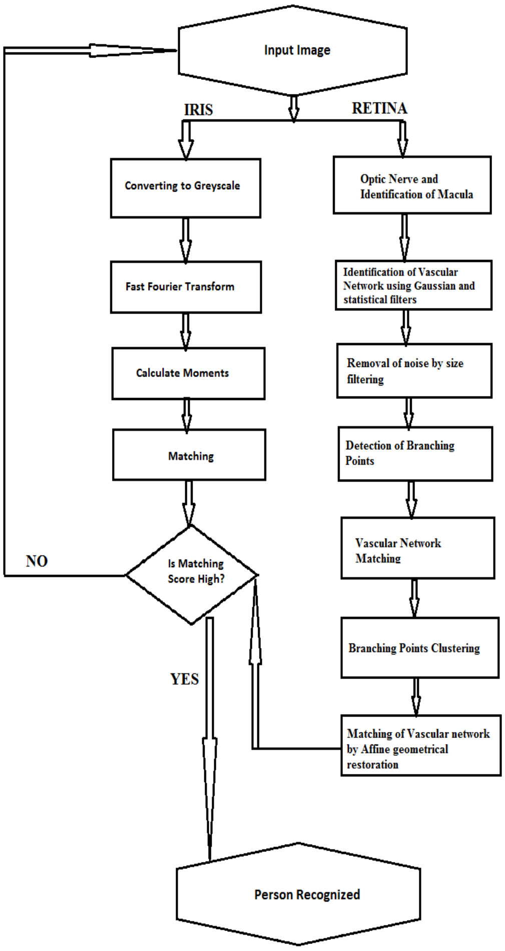
Input Image
IRIS
RETINA
Converting to Greyscale
Fast Fourier Transform
Calculate Moments
Matching
Is Matching Score High?
NO
YES
Optic Nerve and Identification of Macula
Identification of Vascular Network using Gaussian and statistical filters
Removal of noise by size filtering
Detection of Branching Points
Vascular Network Matching
Branching Points Clustering
Matching of Vascular network by Affine geometrical restoration
Person Recognized

Fig.3 Flowchart of Iris and Retina scan

VI. RESULT ANALYSIS

The pros and cons of the proposed system are as follows:
The chief advantage of the Iris and Retina scan is that there are extremely rare chances of incorrect results. This is because no two individuals can have the same retina and iris patterns. So, the percentage of negative result outcomes is almost zero. It is highly reliable. It is very quick, and the uniqueness can be authenticated swiftly. Also, the capillaries in the iris and retina decay too quickly to utilize an amputated eye to get access to the cloud. Also, Retina scanning is considered to be invasive, unlike Iris.
The main disadvantage is that even though the Iris patterns of a person is relatively consistent throughout his/her life, the retina patterns might get altered if they are affected by some sort of disease. So, the individual may not be capable to access the cloud in such cases. The iris scan can be done at a distance, like taking a normal photograph. But for retina scanning, the eye has to be brought close to make sure that the features of the eye are being studied correctly.

VI. CONCLUSION AND FUTURE WORK

Contrary to retina scans, which are used rarely for security purposes in high-level organizations, Iris scans have been implemented at a few places. But these methods are not cost-effective and takes lots of work to get the code running. The Iris scan follows a series of stages, which includes the FFT method. Whereas, the retina scan follows a series of steps which studies the characteristics of the human eye. The dimensions are strictly limited to 512 x 512 pixels. The model recommended is extremely effective, as it is cost-effective as well as easier to implement.
Further developments can be made in case of error detection, wherein a certain authentication method can be developed which may help the system to neglect the false evaluations when the user trying to access it is affected with a disease, that has affected the characteristics of the eye, shrinking or enlarging the features of the same. Also, other profitable procedures can be recommended.

ACKNOWLEDGMENT

We would like to take this opportunity to thank Mrs. S. Kalaiarasi for her continuous support throughout the entire duration of this project. This entire project would not have been possible without the support of Department of Computer Science and Engineering. We gratefully acknowledge SRM Institute of Science and Technology, Ramapuram for providing a platform to pursue this project. The dedication shown by our faculties ensured the completion of this project.

REFERENCES

1. Mohd Danish, Prachi Sharma, “Review study of cloud computing-Benefits, Risk, Challenges and Security”, IRE Journals, Vol.1, Issue 9, pp. 139-142, March 2018. Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., Minkyu Choi, “Biometric Authentication: A Review”, International Journal of u- and e- service, Vol. 2, September 2009.
2. P. Ravi Kumar, P. Herbert Raj, P. Jelciana, “Exploring data security issues and solutions in cloud computing”, in 6th International conference on Smart computing and communications, pp. 691-697,2018.
3. Jun-Song Fu, Yun Liu, Han-Chieh Chao, Bharat K. Bhargava, Zhen-Jiang Zhang, “Secure Data storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing”, IEEE Transactions on Industrial Informatics, Vol.14, No.10, pp. 4519-4528, October 2018.
4. G. Kishore Kumar, Dr. M. Gobi, “Comparative Study on various Biometric Methods Available for Secured Cloud Authentication”, IJARCCE, Vol.6, Issue 9, pp. 162-174, September 2017.
5. Himabindu Vallabhu, R V Satyanarayana, “Biometric Authentication as a service on Cloud: Novel Solution”, International Journal of Soft Computing and Engineering, International Medical Informatics Association (IMIA) and IOS Press, 2019.
6. Samaneh Madanian, Dave Parry, “IoT, Cloud computing and Big data: Integrated framework for healthcare in disasters”, IEEE Transactions on Industrial Informatics, Vol.14, No.10, pp. 4519-4528, October 2018.
7. Muhammad Imran Tariq, “Agent based information security framework for Hybrid cloud computing”, KSII Transactions on Internet and Information Systems, Vol.13, January 2019.
8. Bimi Jain, Dr. M.K. Gupta, Prof. JyotiBharti, “Efficient Iris recognition algorithm using method of moments”, International Journal of Artificial Intelligence and applications, Vol.3, September 2012.
9. Roberto Roizenblatt, Paulo Schor, Fabio Dante, Jaime Roizenblatt, Rubens Belfort Jr, “Iris recognition as a biometric method after cataract surgery”, BioMedical Engineering OnLine 2004.
10. Theodoros S. Petsatodis, Argiris Diamantis, George P. Syrcos, A complete algorithm for Automatic human recognition based on retina vascular network characteristics, Technological Educational Institute of Piracus, Athens, Greece.
11. Li Ma, Tieniu Tan, Yunhong Wang, Dexin Zhang, “Efficient Iris recognition by characterizing key local variations”, IEEE Transactions on Image Processing, Vol. 13, Issue 6, June 2004.

12. G.O. Williams, “Iris Recognition Technology”, 1996 30th Annual International Carnahan Conference on Security Technology, October 1996.
13. C. Sanchez- Avila, R. Sanchez- Reillo, D de Martin- Roche, “Iris based biometric recognition using dyadic wavelet transform”, IEEE Aerospace and Electronic systems Magazine, Vol. 17, Issue 10, October 2002.
14. James R Matey, Oleg Naroditsky, Keith Hanna, Ray Kolczynski, Dominik J. Lolacona, Shakuntala Mangru, Michael Tinker, Thomas M. Zappia, Wenyi Y. Zhao, “Iris on the move: Acquisition of images for Iris recognition in less constrained environments”, Proceedings of IEEE, Vol. 94, Issue 11, November 2006.
15. Renu Bhatia, “Biometrics and face recognition techniques”, International Journal of Advanced research in Computer Science and Software engineering, Vol. 3, Issue 5, May 2013.

AUTHORS PROFILE

S.Kalaiarasi completed her Bachelor of engineering in the field of computer science and engineering from Muthayammal Engineering college. She did her Master degree M.E.-CSE from Sathyabama university in the year 2011. She is pursuing her Ph.D. in SSE, Saveetha Institute of Medical and Technical Science. She is working as an Assistant professor and life member of ISTE. She has great publication records.

Srinidhi Sathyamurthy is currently pursuing her Bachelors of Technology degree as a pre final year student in SRM Institute of Science and Technology, Ramapuram, Chennai, India. Her main research interest includes cloud computing, data science and machine learning.

Tanisha Garg is currently pursuing the degree of Bachelor of Technology in Computer Science and Engineering from SRM Institute of Science and Technology, Ramapuram, Chennai. Her current interest includes cloud computing and web development.

Pallavi Gupta is currently pursuing her Bachelor of Technology in Computer Science and Engineering from SRM Institute of Science and Technology, Ramapuram, Chennai. Her field of interest includes machine learning, robotic process automation and artificial intelligence.