Proc. of the International Conference on Electrical, Computer and Energy Technologies (ICECET 2022)
20-22 July 2022, Prague-Czech Republic

Iris-based Authentication Model in Cloud Environment (IAMCE)

Ethar Abdul Wahhab Hachim
Department of Computer Science
Mustansiriyah University
Baghdad, Iraq
ethar201124@uomustansiriyah.edu.iq

Methaq Talib Gaata
Department of Computer Science
Mustansiriyah University
Baghdad, Iraq
dr.methaq@uomustansiriyah.edu.iq

Thekra Abbas
Department of Computer Science
Mustansiriyah University
Baghdad, Iraq
thekra.abbas@uomustansiriyah.edu.iq

***Abstract*— Biometric identification technology has become increasingly common in our daily lives as the demand for information security and security legislation grows around the world. Together, biometrics and encryption can increase the confidence of the lawful data bearer. In cryptographic systems, key generation is an important topic. As a result, how to use biometrics in cryptographic systems (or bio-cryptosystems) is often tied to how to integrate biometrics with cryptographic "keys". In this paper, since iris recognition is largely considered to be one of the most reliable solutions available we used this metric in order to determine the authorization of persons for using data on the cloud. The Convolution Neural Network (CNN) model for iris images was proposed for the purpose of classifying and identifying authorized and unauthorized persons. Also, the LDA algorithm was used to generate the key from the iris image features. The main idea of key generation is to use it for the purpose of encrypting user data that will be stored in the cloud. In this case, the data of each user will be encrypted depending on the features of his iris. Then, encrypt the generated key using 3DES algorithm. The experimental results of the proposed model show the high accuracy reaching 100% and the encryption efficiency metrics refer to its strength for confronting attacks on data in the cloud.**

Keywords—Biometrics, Iris, Convolution Neural Network (CNN), Cryptography, Authentication, Cloud Computing.

I. INTRODUCTION

Today, the concept of personal identity is becoming increasingly important, and biometrics is a common method of verification that has long been thought to be the most secure and difficult. Biometric systems are evolving technologies that can be utilized in automatic systems to individually and effectively identify persons, making them a viable alternative to older approaches such as passwords [1]. A biometric recognition system has four basic stages in its overall layout. To begin, obtaining a digitalized image of a person using a specialized capturing device is known as biometric trait acquisition. Second, pre-processing allows the acquired image's overall quality to be improved. Third, several algorithms are used to extract the feature data. Finally, in order to accomplish individual recognition, matching of the extracted attributes is commonly used [2].

Many of Deep learning techniques such as transfer learning convolution neural networks and picture augmentation, have been widely used for biometric detection in recent years [3]. A neural network is a set of techniques in which a computer evaluates training models to perform certain functions. It is similar to the neural network in the human brain, in which neurons are called nodes and gather and classify input according to architecture [4]. Biometric cryptosystems necessitate the storage of public data that is biometrically based. This data is referred to as helper data since it is used to retrieve or produce keys. It is not possible to extract keys from biometric data directly due to biometric variance [5]. Acceptance in biometric cryptosystems necessitates the development or retrieval of a hundred percent correct keys, whereas traditional biometric systems only react with "Yes" or "No" [6].

Cloud computing allows users to provide appropriate access to a collection of resources within a network. Many customers use various services to outsource their data to the cloud, reducing the amount of localmemory and the resources required. The storing of sensitive and important data on distant servers, may be highly challenging in a number of privacy-related scenarios, is one of the most severe problems. The use of biometrics guarantees that only authorized persons receive documents from cloud servers [7]. To do this, data processing must be encrypted such that neither the server conducting the processing nor indeed any entity has any access to the data. Furthermore, the processing result should be sent to the customer in encrypted file, with the decryption key only available to the user [8].

The main purpose of this paper is to construct and implement an intelligent cloud trust model based on deep learning to establish trust between users and cloud providers. In addition, using biometrics authentication particularly (iris recognition) allows individuals to use cloud computing successfully and efficiently. This paper is arranged as follows: Section 2 comprise some of the related works. Section 3 explains the theoretical foundation in greater depth. Section 4 shows the proposed system architecture. Section 5 contains the experimental results and security evaluations. Section 6 compares our proposed method with the literature studies. Section 7 has the conclusion.

II. RELATED WORKS

This section is a summary of the most recent advancements in the field of iris recognition. The use of deep learning in this

978-1-6654-7087-2/22/$31.00 ©2022 IEEE

sector is highlighted. These works were arranged in chronological order from oldest to newest as follows:

(K. Priyadarsini and S. Saravankumar, 2018) [9]presented a system for web applications and data administration powered by powerful iris-based biometric authentication. By offering strong authentication, the system ensures the user's identity and provides easy access to data and services.(K. Venkatraman and J. Qaddour, 2018) [10]presented a multilayered security paradigm for access control that included multifactor biometrics authentication. The suggested model employs a randomized approach that employs powerful algorithms for replay protection, session-long authentication, and template update after each successful authentication. (L. Xiulai et al., 2018) [11]presented image encryption and decryption approach depending on the iris characteristic. The iris feature extraction algorithm by using deep learning technique has been built. The characteristics acquired are utilized to perform picture encryption and decryption, and the suggested technique is objectively assessed.(V. Kakkad, M. Patel, and M. Shah, 2019) [12] provided a method employing biometric authentication to secure images on a cloud platform. They introduce the thought of image authentication in two main steps: image compression by using the usual discrete wavelet transform method, and image encryption using a hybrid SHA and blowfish method. This image is then saved in the cloud's database and can be retrieved whenever the user needs.(J. Abu Elreesh and S. Abu-Naser, 2019) [13] suggested an intelligent tutoring method for learning Cloud Network Security depending on a biometrics cryptography system to overcome the majority of security themes notably cloud and network security blunders. Two sets of users, one for teachers and the other for students, rated its simplicity and content.(T. Sudhakar and M. Gavrilova, 2020) [14] introduced a cancelable system's database, biometric engine and deep learning module are all offloaded to the cloud. On the cloud side, CNN with a developed MLP architecture was utilized to extract cross-fold biometric features, which were then converted to templates via random projection for user verification.(Y. Zhuang et al., 2020) [15] aimed to develop a high-precision and efficient iris identification system based on a Convolutional Neural Network (CNN). Deep identification system was trained using iris data from 20 subjects, which included both sides of the eyes. (M. Mihailescu and S. Nita, 2022) [16] suggested a system of three parts (classical authentication, biometric authentication, and searchable encryption).Many domains that need to query data can benefit from it. They've demonstrated that the proposed technique works well for medium to sophisticated network infrastructures. Due to the complexity of the authentication mechanism, this technology provided them with an incredible experience in the cloud environment. (K. Shah, 2022) [17] proposed a deep learning architecture for iris recognition by embedding exponential and rational scaling in fine-tuned pre-trained convolution models ImageNet and VGG19, respectively. The results of the trials suggest that using non-linear scaling improves the performance of the CNN model. The studies were carried out utilizing the MMU iris database. The experimental results show recognition accuracy reached 90%.

III. Methodology

The technologies used in the proposed Iris-based authentication model are discussed in this section.

A. Biometric System

Biometrics is taken from the Greek terms' bio, which means (life) and metrics, which means (to measure). Biometrics' primary function is authentication, allowing only authorized users access [18]. Biometrics is the measurement and statistical analyses of person's behavioral and physical characteristics[19].

- Physiological characteristics: These are a structural characteristics of the human body, "e.g." the face, iris, fingerprints, DNA, or palm.
- Behavioral features: These are a patterns in human actions such as keystrokes, voice, and signatures that are uniquely identifying and measurable.

Biometric systems are divided into two categories these are identification and verification (authentication) [20].

B. Iris Recognition

Iris identification is the technique that distinguishing people depending on the patterns discovered in the ring-shaped area encirclement the pupil of the eye. Iris recognition has attracted alot of interest in a range of security-related businesses in recent years. Iris recognition, like face recognition, is extensively utilized in security-related applications like airports and government buildings for admission and leave. Iris recognition is a technique that is more accurate than other biometric techniques[21].

C. Cloud Computing

The evolution of distributed computing, parallel processing, grid computing, and virtual machines that decide the shape of a new century is referred to as cloud computing. A network or the internet is referred to as the cloud. To look at it another way, the cloud is just something that exists in remote areas. Cloud computing refers to a group of computers and servers that are all connected to the internet and are accessible from anywhere in the world. Cloud computing is on-demand distribution of computer resources such as apps and data centers through the internet for a payment. [22].

D. Biometrics in Cloud Computing

Different strategies can be used to provide cloud security. Authentication is frequently done with passwords. Passwords, on the other hand, are readily cracked. This is the most basic and inexpensive technique. As a consequence, cloud computing may be secured via biometric authentication. Biometric authentication approaches are employed to secure cloud computing [23].

E. TCP/IP Protocol

TCP/IP or Transmission Control Protocol/Internet Protocol is a group of protocols utilized to send data across the internet. It is also commonly utilized on a number of authoritative systems because of its versatility and broad range of value. TCP/IP is now more widely used by Microsoft, which had

previously established its own set of standards. TCP/IP was initially used for transmission and is now used to support many administrations.TCP/IP protocol suite include four levels: Network Interface Layer, Internet Protocol Layer, Transport Layer, and Application Layer [24].

F. Overview of Cryptography

The mathematical art of encrypting and decrypting data is known as cryptography. It allows you to store sensitive data or send it over unsecured networks (such as the Internet) while ensuring that only the intended recipient sees it. Cryptography is the science of encrypting and decrypting secure communication, whereas cryptanalysis is the art of decrypting and assessing secure communication. Traditional cryptanalysis requires analytical thinking, the use of mathematical tools, the finding of patterns, patience, dedication, and chance [25].Cryptography is the combine harvester of mathematical methods with information security components like privacy, the integrity of data, person authentication, and source authentication and authorization. Cryptography is one set of data security strategies, but it is not the only one. There are two kinds of cryptography, the first is called symmetric-key encryption which used one key for both encryption and decryption, and the second is named asymmetric-key encryption which used different keys for encryption and decryption [26].

- Triple DES Algorithm

It is asymmetric cryptography technique that uses cipher blocks. Symmetric cryptography employs the same key to encrypt and decode data. Asymmetric cryptography with a constant or fixed bit size, such as DES's 64 bits, is known as cipher block cryptography. The invention of 3DES is based on a previously known Double DES technique for increasing DES security. The 3DES method requires three keys for both encryption and decryption. The key variants in 3DES can be classified into three groups by using the same key, two different keys, or three distinct keys to each other. 3DES encryption with two or three unique keys is still considered robust for current use [27].

- Salsa(20) Algorithm

Salsa (20) is an encryption stream cipher mode. Salsa's (20) first seed is a 512-bit array, as seen in "Fig. 1".

Constant 1	Key1	Key2	Key3
Key4	Constant 2	Nonce1	Nonce2
Counter1	Counter2	Constant 3	Key5
Key6	Key7	Key8	Constant 4
=			
V0	V1	V2	V3
V4	V5	V6	V7
V8	V9	V10	V11
V12	V13	V14	V15

Fig.1. An array of Salsa (20) distribution [28].

The principal operations of Salsa (20) are (edition, XOR, and rotation) and they are applied to an Array of Salsa (20) for 10 cycles. The Array of Salsa (20) is changed twice per round, thus the name Salsa (20). An addition operation is used at the conclusion of the Salsa (20) between the ultimate adjustment of the Array of Salsa (20) and the starting seed of the Array of Salsa (20) [29].

G. 1D Convolutional Neural Networks (CNN)

In instances when there is little labeled data and substantial signal fluctuations from several sources, 1D CNNs outperform 2D CNNs. The fundamental contrast between 1D and 2D CNNs in both of the kernels and function mappings, 1D arrays replace 2D matrices. The CNN layers learn to extract the features used by the MLP layers in their classification task by evaluating the raw 1D input. As a consequence, the techniques for feature extraction and classification have been combined into a single process that can be modified to increase classification efficiency. Because the only cost-effective approach is the sequence of 1D convolutions, which are just linear weighted sums, one of the most evident advantages of 1D CNNs is their low computing complexity. Convolutional Layers, Pooling Layers, and Fully-connected Layers are the most crucial layers of any CNN [29].

H. Evaluation Metrics

Certain parameters are utilized to determine the system's behavior when evaluating its performance. Metrics are divided into two categories (Classifiers Performance Metrics and Encryption Performance Metrics) as follows [30], [31]:

- Accuracy: The percentage of instances properly classified out of all those presented. It's computed as "Eq. 1":

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FB+FN}} \quad (1)$$

- Precision: For all those identified as class x, the proportion of true x-class occurrences. It is computed as "Eq. 2":

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (2)$$

- Recall: The proportion of instances classified as class x out of all examples classified as class x. It is computed as "Eq. 3":

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (3)$$

- Mean Square Error (MSE): calculates the average square of the "error". In "Eq. 4" the error is determined as the difference between the pixel value of the plain image and the pixel value of the ciphered image.

$$\text{MES} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} [f(i.j)-f`(i.j)]^2}{MN} \quad (4)$$

where M and N are the height and width of the image respectively. $f(i, j)$ is the $(i.j)^{th}$pixel value of the original image, and $f'(\ i,\ j)$ is the $(i.j)^{th}$ pixel value of the decrypted image.

- Peak Signal to Noise Ratio (PSNR): The fidelity of a signal's representation is affected by the ratio between its highest achievable strength and power of corrupting noise. PSNR is often represented in logarithmic decibels, as seen in "Eq. 5"

$$PSNR = \frac{10\log_{10}(2^n-1)^2}{MSE} \quad (5)$$

- RMSE (Root Mean Square Error):The Square of the Root Mean Another form of error measuring approach that is widely used is an error, which is used to quantify the

discrepancies between an estimator's anticipated value and the actual value. It calculates the magnitude of the error as "Eq. 6".

$$\text{RMSE}\ (\hat{\theta}) = \sqrt{MSE\ (\hat{\theta})} \qquad (6)$$

- Normalized Root Mean Square Error (NRMSE): It indicates the relative and absolute inaccuracy between simulated and observed values; the lower the value is the better the performance. It calculates as in "Eq. 7".

$$NRMSE = \frac{RMSE}{\bar{O}} \times 100\% (7)$$

Where $\bar{O}$ is the mean of the observed values.

- Structure Similarity Index Method (SSIM): It is a model that is based on perception. SSIM is expressed as "Eq. 8":

$$SSIM\ (x.y) = [l(x.y)]^{\alpha} \cdot [c(x.y)]^{\beta} \cdot [s(x.y)]^{\gamma} (8)$$

where "l" stands for luminance (used to compare the brightness of two images), "c" stands for contrast (used to compare the ranges between the brightest and darkest regions of two images), and "s" stands for structure (used to compare the local luminance pattern between two images to determine their similarity and dissimilarity), and α, β, and γ are the positive constants.

- Information Entropy Analysis: The degree of randomness or uncertainty in signals can be described using information entropy. The image's information entropy is determined as in "Eq. 9":

$$\text{Entropy} = -\sum_{i=0}^{2^n-1} P(m_i) \log_2 [P(m_i)] \qquad (9)$$

where $P(m_i)$ denotes the occurrence possibility of the gray level i, and i = 0, 1, 2, . . . , 2^n. The 2^n is an image's number of grayscale levels.

IV. The Proposed Method

The proposed (IAMCE) method architecture will be explained in this section. In this procedure, a person is identified by his iris, which is compared to data in the database. The iris images will be processed using the preprocessing procedures outlined above, and then the features will be retrieved using the LDA. For categorization purposes, the features extracted during data processing are encrypted. The person's authorization to access the data is checked when the data is sent to the cloud. The authorization process is carried out using an encrypted key inside data (for example, an image or text) transferred to the cloud through TCP/IP. After entering the data into the iris classifier and ensuring that the person is permitted, the data will be decrypted for iris recognition. The next step is to encrypt the data with the iris algorithm and then save it in the cloud encrypted. The proposed (IAMCE) approach is depicted in "Fig. 2".

A. Dataset Description

This section includes data from the Multi-Media University (MMU) Iris database for Biometric Attendance System training models. IRIS patterns for each eye are unique to each person, making it easier to identify them. There are 460 images in this dataset, comprising five images for each person's iris plus a few empty files.

B. Preprocessing Phase

Image processing is used to extract useful information from images to improve iris images in our proposed system such as transforming RGB Image to Grayscale, enhancing Image using Histogram Equalization, filtering image by Gaussian Filter, apply Image Binarization technique, Iris Image Contouring, find Region of Interest (ROI), Resize Iris Image and Extract Features from Iris Image by Linear Discriminate Analysis (LDA)

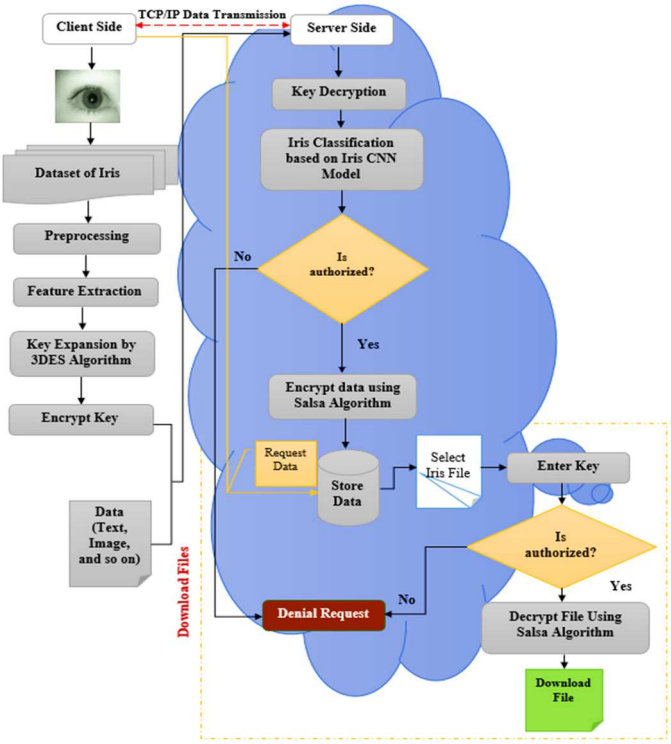

Fig. 2. The architecture of the proposed (IAMCE) method.

As shown in figure 2, on the server-side, all operations are done in reverse so that the user can download the required file.

C. The Proposed Iris CNN Model

The convolution network proposed in this work consists of nineteen layers as shown in "Fig. 3".

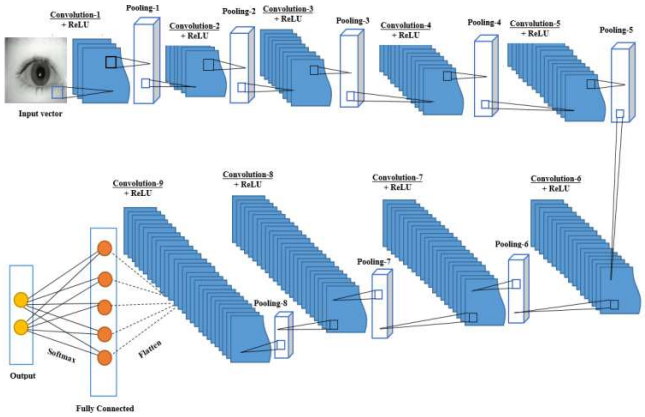

Fig.3. The proposed iris CNN model.

1. Training of Iris Data

Data splitting is the method of splitting available datasets into two halves, commonly for cross-validation aim. The first set of data is utilized to make a prediction model, while the second set is utilized to evaluate the model's results. The bulk of data (70%) goes into the training phase and the remaining data (30%) goes into the testing phase.

2. Testing of Iris Data

The suggested system's testing phase is the second stage. The remaining data (30%) will be handled in the same way as the training data, as previously stated.

Algorithm (1). explain the proposed system phases as follows:

Algorithm (1). Iris-based Authentication Model

Input: MMU Dataset

Output: Accuracy of Iris CNN

Begin

1: Read Iris data

2: Pre-processing Stage

- Convert Color to Gray
- Apply Histogram Equalization
- Apply Image Blurring
- Apply Image Binarization
- Apply Image Countering
- Apply Extract ROI
- Apply Image Resizing

3:Feature Extraction Stageusing LDA.

4: Encrypt Features Using 3DES Algorithm

5: Sending data with the result of the previous step to the cloud.

6: Decrypt data using the 3DES decryption algorithm andapply the Hold-OutCross-Validation method (Splitting Data).

- Results = CNN (Features Set, Targets)
- If the person is authorized, then:
- Encrypt data using the Salsa algorithm and store data in the cloud and go to Step **7**.
- Else
- Go to step **8**.

7:Download files from the cloud

A person must enter his key for verifying then:

If the person is authorized, **then** Download the iris file

Else

Go to step **8**.

End if

8: End

End

V. Experimental Results

The results obtained show the high accuracy of the system, both in terms of recognition and high security of data inside the cloud. Regarding iris recognition, the accuracy of the proposed method was 100%. With regard to the strength of the encryption system, the results according to the standards that were used to measure the strength of the encryption method were very positive as shown in "Table I". "Fig. 4" and "Fig. 5" explains the iris CNN model layers and accuracy result while implementation. We will also compare the results of accuracy with one of the related studies that worked on the same MMU dataset as shown in "Table II".

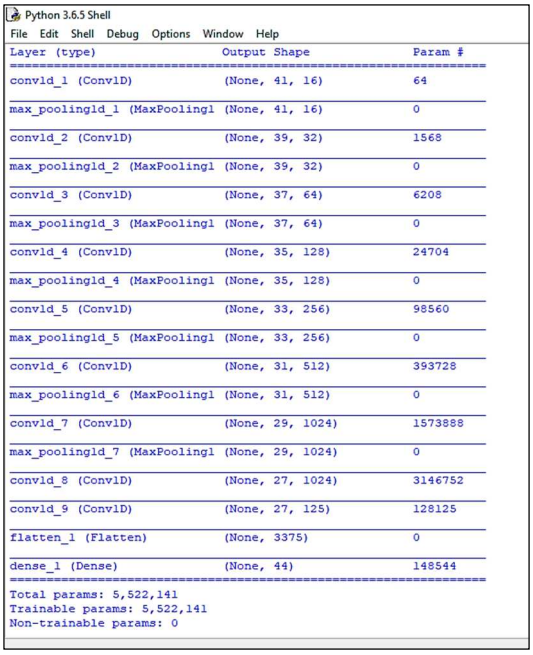

Fig. 4. Iris CNN model

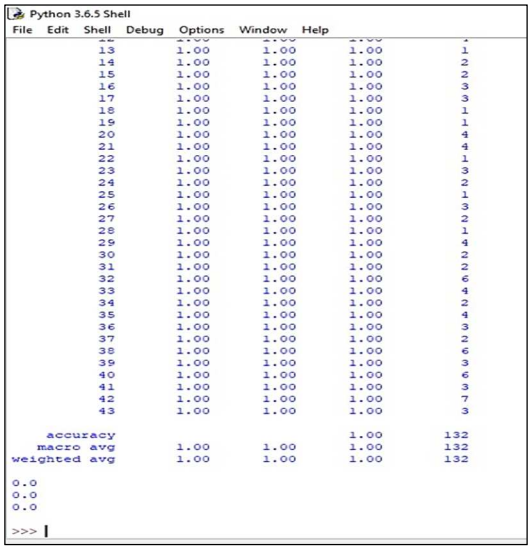

Fig. 5. Accuracy of the proposed method

TABLE I. ENCRYPTION METRICS

Metrics	Value
PSNR	Inf.
SSIM	1.0
MSE	0.0
RMSE	0.0
NRMSE	0.0
Entropy	7.6653

TABLE II. ACCURACY COMPARISON METRICS

Ref. No.	Dataset	Accuracy
[18]	Multi-Media University (MMU) Iris database	90%
Our proposed method	Multi-Media University (MMU) Iris database	100%

VI. Conclusion

It's important in cloud computing that only authorized users have access to the cloud's supplied services. Secure authentication is required for cloud computing to give cloud services to only those users. Traditional authentication methods such as passwords and others are accessible. However, there are some disadvantages: password procedures are not always practicable, passwords can be readily obtained by a hacker, and if a user uses a complex password, the user may forget it, and so on. As a result, biometric authentication approaches are preferable to traditional authentication techniques. Using a biometric authentication solution greatly improves the security level of cloud providers in terms of safe authentication. An iris-based authentication strategy for cloud computing settings is proposed in this paper. We conclude that biometric authentication approaches provide unique ways for authenticating users in cloud computing based on our observations. It also provides a solid platform for future study into cloud computing security.

References

[1] T. Sabhanayagam, V. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," International Journal of Applied Engineering Research, vol. 13, no. 5, pp. 2276-2297, 2018.

[2] T. Murakami, T. Ohki, Y. Kaga, M. Fujio, K. Takahashi, "Cancelable indexing based on low-rank approximation of correlation-invariant random filtering for fast and secure biometric identification," Pattern Recognit Lett, vol. 126, pp. 11–20, 2019.

[3] R. Zemouri, N. Zerhouni, and D. Racoceanu, "Deep learning in the biomedical applications: recent and future status," Applied Sciences, vol. 9, no. 8, 2019.

[4] M. Mahmud, M. Kaiser, A. Hussain, S. Vassanelli, "Applications of deep learning and reinforcement learning to biological data," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, pp. 2063–2079, 2018.

[5] C. Cao et al., "Deep learning and its applicationsin biomedicine," Genom. Proteom. Bioinform, vol. 16, pp. 17–32, 2018.

[6] W. Jones, K. Alasoo, D. Fishman, L. Parts, "Computational biology: deep learning," Emerg. Top. Life Sci. , vol. 1, pp. 257–274, 2017.

[7] P. Govindaraj and N. Jaisankar, "A review on various trust models in a cloud environment," Journal of Engineering Science and Technology Review, vol.10, no. 2, pp. 213- 219, 2017.

[8] V. Balaram, "Cloud computing authentication techniques: a survey," International Journal of Scientific Engineering and Technology Research, vol. 6, no. 3, pp. 0458-0464, January-2017.

[9] K. Priyadarsini and S. Saravankumar, "Amalgamation of iris biometrics and cryptography in cloud computing for improved authentication," Journal of Engineering and Applied Sciences, vol. 13, no. 8, 2018.

[10] K. Venkatraman and J. Qaddour, "Multilayered cloud security model using multifactor session-long biometrics access control," International Journal of Computer Science and Telecommunications vol. 9, no. 1, January 2018.

[11] L. Xiulai, J. Yirui, C. Mingrui, and L. Fang, "Research on iris image encryption based on deep learning," EURASIP Journal on Image and Video Processing, 2018.

[12] V. Kakkad, M. Patel, M. Shah, "Biometric authentication and image encryption for image security in cloud framework," Multiscale and Multidisciplinary Modeling, Experiments, and Design, 2019.

[13] J. Abu Elreesh and S.Abu-Naser, "Cloud network security based on biometrics cryptography intelligent tutoring system," International Journal of Academic Information Systems Research (IJAISR), vol. 3 no. 3, pp. 37-70, March – 2019.

[14] T. Sudhakar, M. Gavrilova, "Cancelable biometrics using deep learning as a cloud service," IEEE Access, June 19, 2020.

[15] Y. Zhuang, J. Chuah, C. Chow, and M. Guozong, "Iris recognition using convolutional neural network," 2020 IEEE 10th International Conference on System Engineering and Technology (ICSET), 9 November 2020, Shah Alam, Malaysia.

[16] M. Mihailescu and S. Nita, "A searchable encryption scheme with biometric authentication and authorization for cloud environments," Cryptography, vol. 6, no. 8, 2022.

[17] K. Shah, "On human iris recognition for biometric identification based on various convolution neural networks," Ph.D. Thesis, Computer Science Department, Gujarat Technological University, January 2022.

[18] D. Verma and S. Ojha, "Performance analysis of biometric systems: a security perspective," International Journal of Advanced Research in Computer and Communication Engineering, vol. 8, No. 4, April 2019.

[19] C. Jamdar, A. Boke, "Person Identification system using multi-model Biometric Based on Face," International Journal of Science, Engineering and Technology Research(IJSETR), vol.6, pp.628, April 2017.

[20] S. Idrus, "Soft biometrics for keystroke dynamics," Ph.D. thesis, Computer Vision and Pattern Recognition, Universite de Caen Basse-Normandie, 2014.

[21] H. Rana, S. Azam, R. Akhtar, J. Quinn, and M. Moni, "A fast iris recognition system through optimum feature extraction," PeerJ Computer Science Journal, 2019.

[22] Z. Dingyu, "Cloud computing technology and its application in robot control," IOP Conf. Series: Materials Science and Engineering, vol. 392, 2018.

[23] A. Hussein, H. Abbas, and M. Mostafa, "Biometric-based authentication techniques for securing cloud computing data - a survey," International Journal of Computer Applications, vol. 179 – no.23, February 2018.

[24] A. Pande and S. Devane, "Study and analysis of different TCP variants," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16-18 Aug. 2018.

[25] S. Kumar, A. Mishra, G. Karnani, and M. Gaur, "Cloud security using hybrid cryptography algorithms," International Conference on Intelligent Engineering and Management (ICIEM), 2021.

[26] D. Nanda and S. Sharma, "Security in cloud computing using cryptographic techniques", International Journal of Computer Science and Technology, vol. 8, no. 2, 2017.

[27] M. Abdul Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish for guessing attacks prevention," Journal of Computer Science Applications and Information Technology, August 10, 2018.

[28] H. Najm, H. Hoomod, R. Hassan, "A proposed hybrid cryptography algorithm based on GOST and salsa (20)," Periodicals of Engineering and Natural Sciences, Vol. 8, No. 3, September 2020, pp.1829-1835.

[29] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj, and D. Inman, "1D convolutional neural networks and applications: A survey," Mechanical Systems and Signal Processing, Volume 151, April 2021.

[30] M. Grandini, E. Bagli and G. Visani, "Metrics for multi-class classification: an overview", arXiv:2008.05756v1 [stat.ML] 13 Aug 2020.

[31] U. Sara, M. Akter, and M. Uddin, "Image quality assessment through FSIM, SSIM, MSE, and PSNR—a comparative study". Journal of Computer and Communications, vol. 7, pp. 8-18, 2019