ISSN 2347 - 3983
Volume 8. No. 8, August 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter37882020.pdf
https://doi.org/10.30534/ijeter/2020/37882020

# An Efficient Siamese Network Based Multi-Biometric Key Distribution Protocol for Cloud Data Security

**Ruth Ramya Kalangi[1], Dr. M.V.P. Chandra Sekhara Rao[2]**
[1] Research Scholar, Acharya Nagarjuna University, Namburu, India, ramya_cse@kluniversity.in
[2] Professor, RVR & JC College of Engineering, Chowdavaram,India, manukondach@gmail.com

## ABSTRACT

Storage as a Service is one of the functionalities of cloud computing. Storing data in cloud has its own advantages such as high availability, low costs etc., but also disadvantages like improper authentication. Features extracted from single type of biometrics of users are used to serve this purpose. Limitations of using single type of biometric systems include insecure key distribution, high computational time and memory. They are applicable only to structured data with limited data size. To overcome all these disadvantages multiple types of biometrics of users came into existence. Feature extraction, key generation, encrypting cloud data and key distribution is difficult task for many applications as the number of biometrics considered per user increased. To overcome all these limitations an efficient Siamese Network based Multi-Biometric (SNMB) model is proposed. In this work, an authentication based deep learning framework is proposed to improve the feature selection process and error rate on the different biometric feature sets also, a novel key distribution model is implemented to secure the secret of the cloud user for strong data security. Experimental results prove that proposed SNMB model has less computational time and memory. Experimental results are tested on different biometric images and the performance of the proposed SNMB model has better computation time (~6%) and less memory consumption (4%) than the conventional cloud security models.

**Key words**: Attribute based encryption, Cloud Data Security, Key Distribution, Multi-Biometrics, Siamese Network.

## 1. INTRODUCTION

A biometric system is defined as a system that automatically recognizes a person based on certain inherent physiological or behavioral characteristics through a combination of material recognition and model algorithms. Since, biometric system requires an individual presence at the time of identification, false claims of repudiation can be greatly avoided [1]. However, as features associated with biometric characteristics are unique to an individual multiple identities will not be generated. In modern digital society, daily activities such as accessing protected applications, gaining access to personal digital devices, databases or receiving financial services require an individual to be authorized by providing identification [2]. Service providers use the identification or authentication method to define (determine or verify) an individual identity to grant permission [2].

Today, as computers are used to perform medical assessments it is becoming increasingly important to develop computer-aided recognition systems for people. Knowledge and token-based approaches are the two conventional approaches used to identify individuals until the last few years. Individuals can easily deny communicating with the recognition system by pretending to have stolen their code [3]. They can also hide their true identity by displaying forged documents of identification. Therefore, traditional approaches are not enough to identify identity and there is a need for stronger systems focused on "what you are" called biometrics [4]. Biometric systems have therefore emerged as a new solution to meet the ever-increasing demand from our society for enhanced security requirements in order to meet the requirements of recognition systems. Using multiple biometrics of user is more advanced to ensure improved accuracy; (ii) Secondary means of enrolment and authentication or identification where appropriate data are not collected from a biometric sample; and (iii) spoofing attempts can be detected by non-live sources of data such as fake fingerprints. Most of the existing works are based on extracting maximum and minimum local values from the entire contour of the side. Feature extraction methods must be accurate in finding different texture structures from an image, and the computational complexity must be low in order to maintain the features in various applications [5,22].

Earlier features from biometrics are extracted using traditional approaches like crossing number algorithm etc., Now-a-days biometric features are extracted using deep learning networks like CNN etc., The main objective of

implementing models of artificial neural networks is used as they are effective and has optimal architecture for classification and selection of features. This work mainly focuses on using a Siamese Network (SNN). The experimental work gave a good result in ranking the attributes by constructing a SNN model. SNN's traditional classification concept has transformed into a modern approach for extracting features. Handling huge amounts of data with multiple class entities can only be classified with a network of multiple layers. The SNN models are trained with batch gradient back propagation in a completely supervised way. The parameters are tuned and optimized to achieve a better type of build [6]. The main task of the convolutional layer is to detect the local conjunctions of entities from the previous layer and map their appearance on a feature map. The image is divided into perceptions as a result of convolution in neural networks, creating local receptive fields and finally compressing perceptions in the characteristic maps.

Traditionally, secrete key generation is a software program which generates a secure cryptographic key derived from biometric data. Encryption and decryption are performed by symmetric cryptographic algorithms using the secret key [7,23]. Another use of the secret key is to generate message authentication codes to provide data integrity. Key Distribution protocols are designed to manage network members easily and for secure communication. Most of the traditional key distribution protocols are classified as core centralized, distributed or decentralized. Securely distributing secret key is of major concern. It can be done only when a trusted third party is involved or if it is encrypted and distributed. Public key is distributed using PKC [8]. Proposed Trusted Cloud Server based Key Distribution Protocol (TCSKD) is a decentralized protocol.

Key binding systems are systems that connect the biometric model with a randomly generated cryptographic key that is released to the user. It is possible to use more than 250 distinctive iris characteristics (degrees of freedom) in biometrics, resulting in six times more identifiers than the fingerprint. Most of the recognition systems proposed in the biometric literature provide a defined safety level. These systems performance is not adaptive to meet the safety level requirement [9, 10].

Gomez et. al., [11] collected hand pictures from 170 people using a CCD camera for hand placement without any features. Fei et. al., [12] used a flatbed scanner to capture hand images from 50 people. The middle finger's central line is known to be the key axis in finding the ROI palm print. The palm area receives a fixed size ROI. Gomez et. al., [13] uses a scanner interface to capture manual images.

Two midpoints, one in the index finger region at the bottom of the finger and one in the small finger region at the bottom of the finger, form the baseline. W.Y. Han et. al., [14] used radial distance from the middle of the wrist to find the valley points between the fingertips and the tip points of the fingers. Line detection methods commonly extract lines using edge detectors to match two palm print images directly or represented in other formats.

V. I. Ivanov et. al., [15] proposed finite randon transformation, canny edge detector, modified finite radon transformation, sequential gradient-related filtering operations, morphological operators and steerable filters are used to remove main lines. Recognition based solely on main lines fails to perform well when more people are enrolled in the recognition systems due to this feature's uniqueness across the population. In the subspace, computed coefficients are known to be characteristics used for identification. By using PCA, N. Hu, H.et. al., [16] suggested an approach for feature extraction. The Karhunen-loeve transformation technique is used to project the palm print image into a feature space of relatively low dimensions called Eigen palms.

G. Jaswal et. al., [17] used a similar technique to use Fisher linear discriminate to project the palm print images to minimize the space of the dimensional feature called the fisher palm. Independent Element Analysis was used by L. Shang et al., [18] to determine palm printing features. L. In order to obtain palm printing functionality, Shang used Locality Preserving Projection process because subspace is designed on the basis of training data; it needs to be retrained if the recognition system is enrolled by new people.

G. Jaswal et.al., [19] used coding-based method to encode filter bank responses into bitwise function code. They implemented a method of palm code using a Gabor filter to extract local palm print phase data.

The methods of radon conversion and hair wavelet are used by Kaur et. al., [20] to remove features. Features derived from the middle and ring finger, the multi matcher solution is proposed. During registration, hash key is allocated to each client and bio hashing technique is used in the matching process.

The main objective of this paper is to develop a hybrid cloud based key distribution protocol using the multiple biometrics and cloud data security algorithms. This paper proposes an efficient Siamese Network based Multi-Biometric (SNMB) model. This model extracts features from multiple biometrics of a single user using a deep learning network called Siamese and thus extracted features are integrated/concatenated and a hash value is calculated using Improved Adaptive Integrity Algorithm (IAIA). Extracted hash value can be used as a key

for encrypting and decrypting cloud data using Improved Multi Biometric Ciphertext Policy Attribute based Encryption algorithm (IMBCP-ABE). Moreover, a secure key distribution protocol called Trusted Cloud Server based Key Distribution Protocol (TCSKD) was developed for distributing secret/private key to cloud user for decrypting the data stored in cloud. Results and discussion are given in Section 3. Conclusion and recommendations are made in the last section.

## 2. PROPOSED SIAMESE NETWORK BASED MULTI-BIOMETRIC MODEL (SNMB)

The overall framework of the proposed Siamese Network based Multi-Biometric Model (SNMB) for cloud data security is illustrated in Figure 1. Three types of biometrics such as Iris, Fingerprint and Face recognition are taken as input. Features are extracted from the above mentioned biometrics individually using Siamese Network. Features thus extracted from Iris, Fingerprint and Facial recognition are integrated or fused which is called as biokey. Biokey can be hashed so that the resulting hash value or the message digest thus generated can be used for data integrity and can also be used as key for encrypting data stored in cloud server using IMBCP-ABE algorithm. In IMBCP-ABE algorithm policies are built on hash values calculated on multiple types of biometrics collected from multiple users. A new Key Distribution Protocol called Trusted Cloud Server based Key Distribution Protocol (TCSKD) is designed for distributing secret key securely for decrypting data stored in cloud by cloud users. Proposed SNMB model is divided into 5 phases.

i. Feature Extraction from multiple biometrics of users using Siamese Network.
ii.Key Generation using Improved Adaptive Integrity Algorithm (IAIA).
iii. Encrypting Cloud Data by cloud owner using IMBCP-ABE Algorithm.
iv. Key Distribution using proposed TCSKD protocol.
v. Decrypting Cloud Data using IMBCP-ABE algorithm by cloud user.

### 2.1 Feature Extraction from Multiple Biometrics of User using Siamese Network

Features from biometrics are extracted using Siamese networks. A deep neural network (DNN) framework implemented on line data and can accomplish control and decision-making steps within the system. Most of these systems are based on a convolutional neural network (CNN) which can use convolutional layers as an entity extractor to create input image entity maps. Convnets are a neural subset of interlayer-limited connections. Neural networks are not sufficient to scale full pictures. They can also contribute to excess. CNN handles two input pixels differently depending on their proximity or size, which allows use of local characteristics. Various images can be categorized with the help of CNN using the features in the image. In the intermediate layers of the current CNN model, kernels of various sizes are used. Initially, a random value is added for every kernel. The kernel values are modified at each point to remove the input image functionality. Following a convolution layer, a pooling layer is introduced. It reduces the space data. The function dimensions are the, and parameter reductions monitor the overlay, and measurements are done to make the network unchangeable from slight adjustments and distortions. Total linked layers are added after convolutionary and pooling layers. Here the neurons of the current layer are linked to all activation of the previous layer. The multiplication of the matrix is done along with an offset bias. A drop-off function is used in such a layer to decrease the over-fitting and total number of parameters. A function like this is extracted through convolution operations when the kernel is known for a certain feature. There is no awareness of the number or existence of the apps. Consequently, the convolution operation does not exhaust the function. With propagation of transmission, characteristics are devalued with convolution, then sequentially corrected with back propagation. Once the training is complete, most kernels should be stabilized by reducing errors.

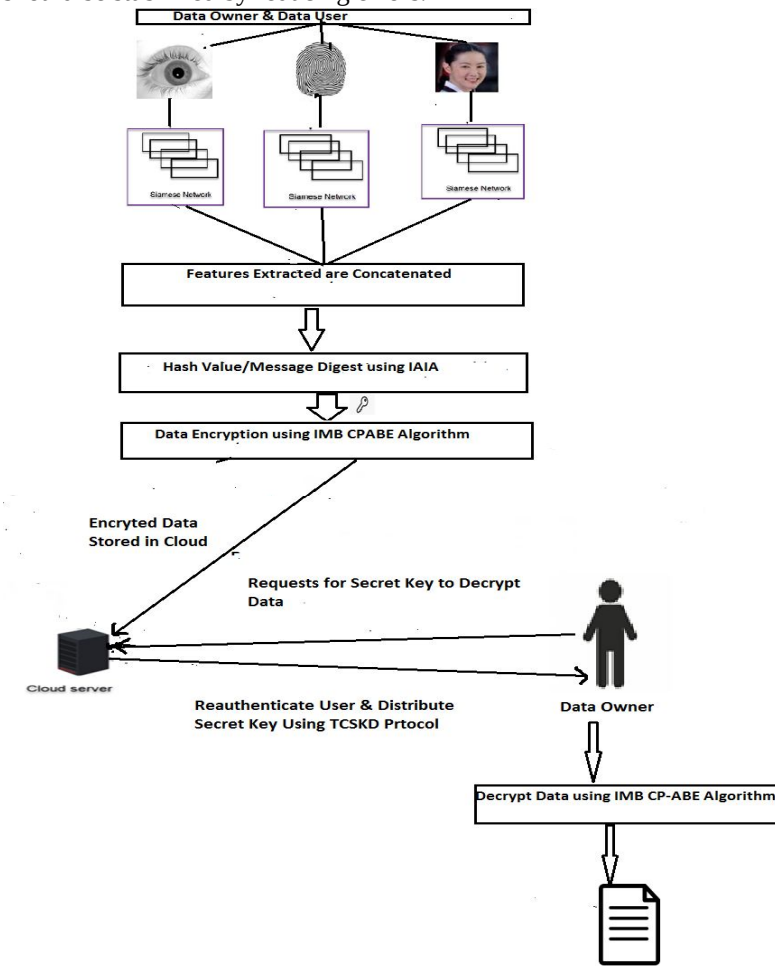


**Figure 1 :** Overall Design Framework for Siamese Network based Multi-Biometric Model (SNMB) for Cloud Data Security

This means that the CNN convolution layer plays the role of local filters on the input space and the weights of the filter kernel calculated during the learning process [3]. The convolution layers supress the receiving fields of the hidden layers to be local, which, thanks to the convolutional layers, make it possible to extract the local characteristics. On the other hand, the memory requirements as well as the computational complexity are reduced due to the CNN structures. But with applications processing local correlation inputs such as images and videos, CNN can achieve greater efficiency. In CNN, a sequence of convolution and grouping operations was performed on the input image for the feature extraction process. The transmission process is illustrated in Figure 2 only for fingerprint similarly its possible for iris and face. Airs of pixels are introduced into a one-dimensional CNN to extract features. Then, a fully connected network concatenates two entities and maps the entities to the output.

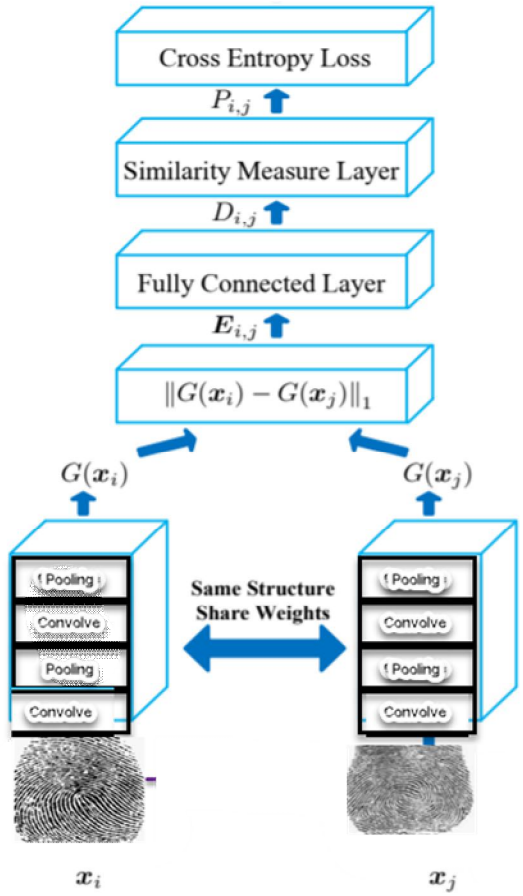


**Figure 2:** Siamese Network

A Siamese network can also be used for the purpose of authentication. A Siamese network is a neural network architecture that takes two inputs instead of one and calculates a metric from those inputs. The idea is to have two identical input networks acting as layers of encoding, which can then be merged and fed into one output network. Weights must be modified identically for both input networks, in order to have two equivalent encoding networks. A Siamese network learns how to extract interesting and diverse features from inputs that can then be used to form a vector representing input information. Encoded vectors can then be used to calculate a metric based on the encoded semantic information stored in the vectors in the output network. The use of convolution neural networks as part of Siamese network due to their ability to extract possibly very diverse features and lower parameters compared to a fully connected neural network. The filtering design of convolution layers, where a single kernel is used for all regions of an image, often improves the invariance of translation to the input data as shown in figure 3(a), (b), (c).

$$E_t = -\frac{1}{N}\sum_j f_j.\log(f_j) \quad \text{---(1)}$$

$$P(f_1, f_2) = \frac{1}{2}(1 - E_t)^2 \quad \text{---(2)}$$

$$N(f_1, f_2) = \begin{cases} E^2_t & \text{if } E_t < \lambda \\ 0 & \text{else} \end{cases} \quad \text{---(3)}$$

$$\frac{\partial E_{ti}}{\partial f_m} = -\sum_k E_{tik}\frac{\partial \log E_t}{\partial f_m}$$

$$= -\sum_k E_{tik}\frac{1}{E_t}\frac{\partial E_{tk}}{\partial f_m}$$

$$= -\sum_{k=m} E_{tik}\frac{1}{E_{tk}}E_{tk}(1 - E_{tk}) + \sum_{k\neq m} E_{ti,k}\frac{1}{E_{tk}}E_{tk}E_{tm} \quad \text{---(4)}$$

where $E_t$ is the entropy of the feature, $f_j \in F, \lambda$ is threshold,

$P(f_1, f_2)$ is the positive feature set.

$N(f_1, f_2)$ is the negative feature set.

In the Equation 1, the entropy of the features is computed to check the essential features in the large number of feature space. Equation 2 represents the positive class feature extraction by using the entropy function. Equation 3 represents the negative class feature extraction on the large feature space. Here, threshold is used to filter the negative bag features in the feature space. Equation 4 is the partial derivative of the entropy function for error rate estimation process.

Moreover, even the Siamese Neural Network architecture has been used extensively in the field of k-shot learning by exploiting the power of convolution models to generalize not only new data but also data from different distributions on the predictive powers. Siamese networks are based on the idea that we can connect two or more neural networks in such a way as to share some of their weights. The resulting network may have multiple independent inputs and outputs, and multiple parts make up its loss function. An example of such a network is a combination of auto encoder and classifier when

trying to reduce data dimensions so that the compressed representation will still contain the information that helps us to distinguish between classes.

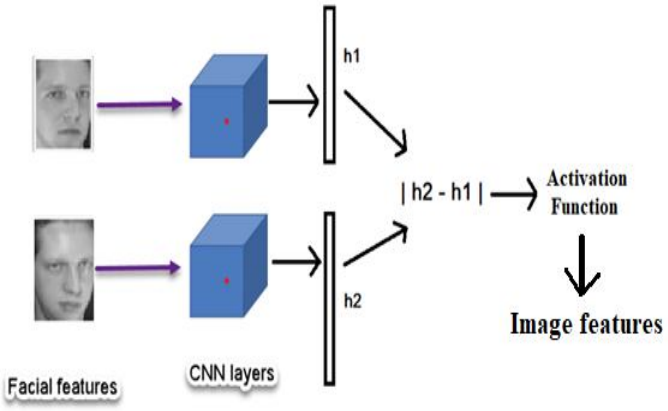


**Figure 3(a) :** Siamese Network based Facial Features Comparison

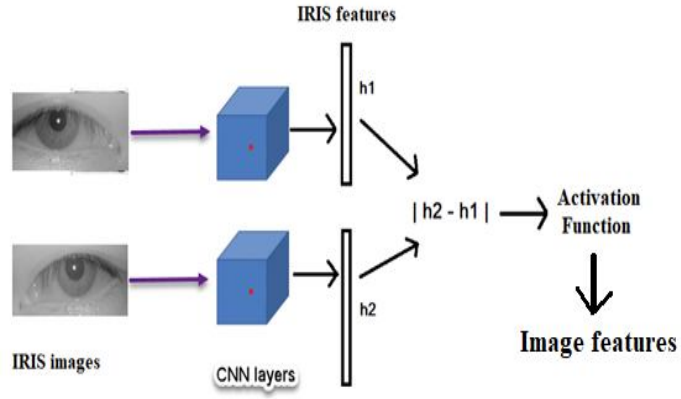


**Figure 3(b) :** Siamese Network based Iris Features Comparison

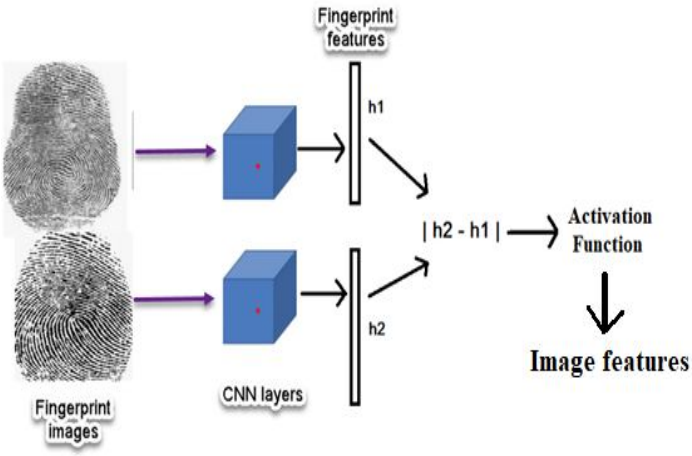


**Figure 3(c) :** Siamese network-based Fingerprint Features Comparison

### 2.2 Key Generation using Improved Adaptive Integrity Algorithm (IAIA)

Features extracted from three types of biometrics i.e., Iris, Fingerprint and Facial recognition are integrated or concatenated and given as input to Improved adaptive integrity algorithm IAIA. The only difference between AIA and IAIA algorithm is that in AIA algorithm minutiae extracted from fingerprint is the only input to be considered but in IAIA algorithm we consider features extracted from Iris, fingerprint and face as Input [20]. The hash code generated by IAIA algorithm is used as biokey. Thus generated biokey can be used as key for encrypting the data stored in cloud and also can be used in distributing secret keys securely to cloud users.

### 2.3 Encrypting Cloud Data by cloud owner using IMBCP-ABE Algorithm

Data to be stored in cloud is encrypted using IMBCP-ABE algorithm. The only difference between ICP-ABE and IMBCP-ABE algorithm is that in ICP-ABE algorithm hash value calculated on minutiae extracted from fingerprint is the only input to be considered but in IMBCP-ABE algorithm we consider hash value calculated on features extracted from Iris, fingerprint and face as Input [21]. Algorithm 1 illustrates the steps in IMBCP-ABE algorithm in brief. Input to algorithm 1 include Multi-biokey, Multi-biokey Hash H (MBK), Attributes set A= {MBK (1),MBK (2),MBK(3)…MBK(n)}, Policies are constructed by using hash values generated from multiple biometrics of users. P={H(MBK(1))and H(MBK(2)) and H(MBK(3)) and…and H(MBK(n)), KD, H(KD)} and output is ciphertext.

**Algorithm 1:** Improved Multi Biokey Ciphertext Attribute Based Encryption Algorithm IMBCP-ABE

**Step 1 Multi-biokey Setup:** ICP-ABE parameters are initialized. Master key and public key are generated using hash value generated from multi-biometric features.

**Step 2 Multi-biokey Encryption Phase:** Cloud user attributes and their unique policies are taken as inut and generate encrypted text as output. Each attribute represents the user multi-biokey and the policies represent the hash of the multi-biokey. The encryption algorithm encrypts the message M using a tree structure with polynomial access T.

**Step 3 Multi-biokey Key Generation:** Set of attributes and hash value produced out of multiple biometric features called as biokey are input and secret key is output. These keys are used to access the data and to improve the confidentiality of secret key distribution during decryption phase.

### 2.4 Key Distribution using Proposed TCSKD Protocol

A secret key is generated at the cloud server for each user to access data. This secret key is generated by using the user's registered cloud instance ID that is unique to each trusted cloud server and used in data decryption process. Notations

used in TCSKD protocol are denoted in table 1. TCSKD protocol is illustrated in protocol 1.

**Table 1:** Notations used in TCSKD Protocol

| Notation | Description |
|---|---|
| U(i) | $i^{th}$ user biometric identity |
| k | User defined value |
| BKUID | Biometric key for user identities |
| m | Chaotic random number |
| n | Number of biometric identities |
| $C_n(r)$ | [0,ChatoicRandom] |
| $g^n$ & $g^m$ | generators |
| ρ | Prime integer from cyclic group |

**Protocol 1 :** Trusted Cloud Server based Key Distribution Protocol (TCSKD)

---

**Step1**. Each cloud user enters their unique identity for communicating with cloud server. This unique identity is sent to cloud users using either SMS or Email-ID.

**Step 2.** Generate unique credentials as

GetBytes MB=MultiKey(U(i));// ith user multi-biometric key

BKUID=Decimal(MB)%k// where k is user defined constant.

i.Cloud user P selects a chaotic random number m m ∈ [0,ChaoticRandom]

ii. Cloud user P evaluates $g^m$ mod ρ and sends it to cloud server KDC.

iii.Cloud server KDC selects a random chaotic n, n ∈ [0, ChaoticRandom]

iv.KDC computes $g^m$ mod ρ and sends it to cloud user .

v.Cloud user P computes key distribution KD=( $g^m$)$^n$ mod ρ and KDC computes KD=( $g^m$)$^n$ mod ρ.

**Step 3**. Cloud user request key to the KDC.

**Step 4.** KDC generates key KD.

**Step 5**. In steps 3 to 6, KDC generates key and sends it to the requested cloud user. KDC sends (KD|| InstanceID: CID) to cloud user for data decryption.

---

### 2.5 Decrypting Cloud Data using IMBCP-ABE Algorithm by Cloud User

Cloud users whoever want to access data sends a request to cloud server. Cloud server verifies whether the cloud user is authenticated or not and distributes secret key used for decryption in a secure manner using TCSKD protocol to cloud user. Using secret key cloud user will be able to decrypt the data.

## 3. EXPERIMENTAL RESULTS

Amazon cloud storage and computing services are used for data encryption and decryption process. In the Amazon AWS environment, different types of users and different cloud instances are used to generate key based on the multiple biometrics features. Several parameters such as data size, sensitivity, runtime, user policies are used to verify the efficiency of the proposed model compared to the existing models. Figure 4(a), 4(b) & 4(c) describes various biometrics (Iris, Fingerprint & Face Recognition) of n user.

**Figure 4 :** (a) Sample Iris Image, (b) Fingerprint Image, (c) Facial Image

Features extracted from Iris, Minutiae extracted from Fingerprint & Features extracted from face using Siamese Network are represented in Figure 5(a), (b) & (c).

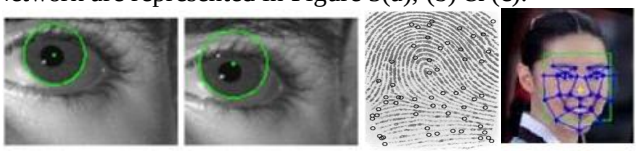

**Figure 5 : (a)** Features Extracted from Iris**, (b)** Minutiae Extracted from Fingerprint & **(c)** Features extracted from Face using Siamese Network

Table 2 compares the number of bits that would be affected when a single input bit is changed in the proposed AIA algorithm when multiple biometrics of multiple users are considered for calculating hash value. It is also observed from table that proposed IAIA algorithm exhibits higher sensitivity.

**Table 2 :** Compares Bit Sensitivity of Proposed algorithm IAIA with Existing Algorithms when Multiple Biometrics of Multiple Users were Considered for Calculating Hash Value.

| No. of Users | SHA256 | SHA512 | MD5 | Linear Chaotic | AIA | IAIA |
|---|---|---|---|---|---|---|
| **1** | 121 | 129 | 123 | 131 | 133 | 144 |
| **2** | 124 | 121 | 127 | 126 | 135 | 149 |
| **3** | 133 | 130 | 134 | 131 | 136 | 145 |
| **4** | 135 | 125 | 130 | 130 | 138 | 138 |
| **5** | 113 | 130 | 134 | 130 | 142 | 140 |
| **6** | 130 | 121 | 113 | 119 | 136 | 148 |
| **7** | 121 | 125 | 131 | 131 | 139 | 142 |
| **8** | 121 | 114 | 132 | 123 | 140 | 137 |
| **9** | 123 | 114 | 116 | 127 | 18 | 144 |
| **10** | 128 | 130 | 124 | 124 | 136 | 144 |

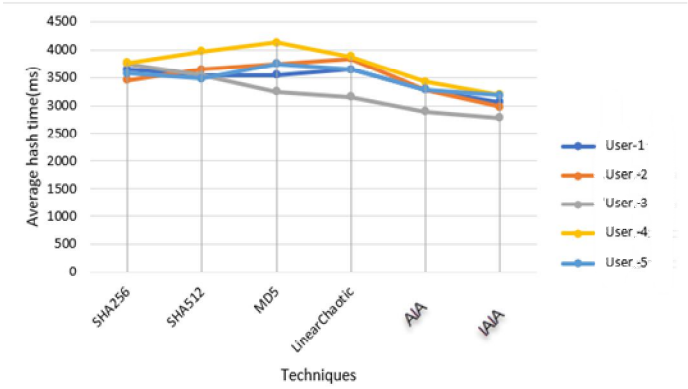


**Figure 6** : Comparison of Average Runtime of Proposed IAIA Algorithm with Existing Algorithms when Multiple Biometrics of Users was considered (Hash size=2048 bits)

Figure 6 compares average runtime in milliseconds of the proposed IAIA algorithm to the existing hash algorithms against number of cloud users. From this figure, it can be inferred that average runtime of IAIA algorithm is less when compared to existing algorithms.

Table 3 compares average encryption time in milliseconds of the proposed **IMBCP-ABE** algorithm to the existing encryption algorithms with respect to various data sizes. From this table, it can be inferred that average encryption runtime of **IMBCP-ABE** algorithm is less when compared to existing algorithms.

**Table 3** : Comparison of Average Time taken to Encrypt Data using Proposed IMBCP-ABE Encryption Algorithm with Existing Algorithms with respect to Data Size in Milliseconds

| Data Size | CPABE | KPABE | ICP-ABE | IMBCP-ABE |
|---|---|---|---|---|
| **10MB** | 4691 | 4681 | 3541 | 3194 |
| **20MB** | 4843 | 4649 | 3635 | 3179 |
| **30MB** | 4613 | 4804 | 3490 | 3139 |
| **40MB** | 4752 | 4355 | 3519 | 3280 |
| **50MB** | 3929 | 4737 | 3556 | 3145 |
| **60MB** | 4285 | 4284 | 3566 | 3179 |
| **70MB** | 4240 | 4536 | 3526 | 3207 |
| **80MB** | 4858 | 3991 | 3623 | 3280 |
| **90MB** | 3838 | 4206 | 3525 | 3219 |
| **100MB** | 4016 | 4146 | 3531 | 3114 |

Figure 7 compares memory occupied by IMBCP-ABE algorithm with existing algorithms with respect to various data sizes. From this figure, it can be inferred that memory occupied by IMBCP-ABE algorithm is less.

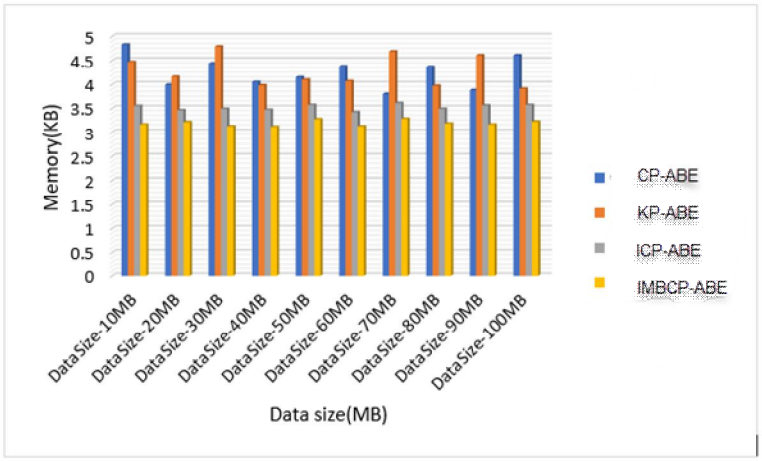


**Figure 7** : Comparison of Memory occupied by Proposed ICMBCP-ABE Algorithm with Existing Algorithms with respect to Various Data Sizes

Figure 8 illustrates memory occupied by proposed TCSKD protocol used in SNMB model with existing models for cloud data security. From the figure, it is observed that proposed TCSKD protocol occupies less space when compared to other algorithms.

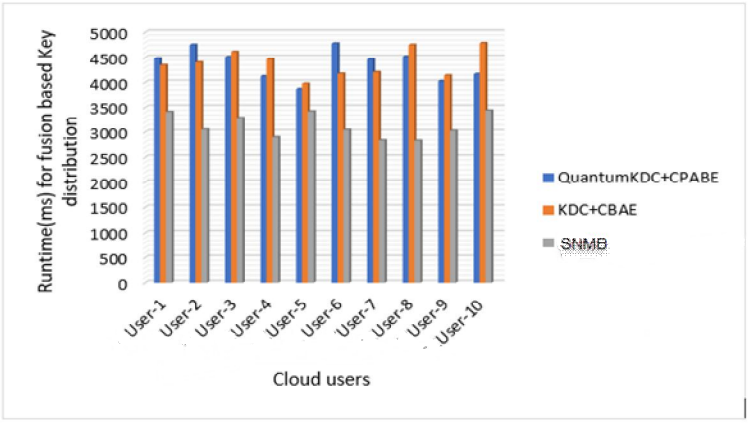


**Figure 8:** Comparison of TCSKD protocol used in SNMB Model with Existing Models for Cloud Data Security

## 4. CONCLUSION

This paper considers Iris, Fingerprint and Face as biometrics from multiple users. Features from the above mentioned biometrics are extracted using a deep learning framework called Siamese Network. The advantage of using Siamese network is it can be used for extracting features from biometrics and also for the purpose of authentication. Extracted features from multiple users are concatenated and hash value is calculated. Hash value acts as key for encrypting data using IMCCPABE algorithm that is to be stored in cloud server. Data users who want to access the encrypted data need a secret key in order to decrypt it. So, Cloud server distributes secret key using proposed TCSKD protocol to Data user in a secure way. The experimental results prove that proposed

SNMB model achieved better performance than the traditional key distribution models in terms of time and data storage. Experimental results are tested on different biometric images and the performance of the proposed SNMB model has better computation time(~6%) and less memory(4%) than the conventional cloud security models.

**ACKNOWLEDGEMENT**

**1. Mrs. Ruth Ramya Kalangi** is a Research Scholar in the department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. She is currently Assistant Professor in the department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. Her research interests are Biometrics, Network Security and Wireless Sensor Networks.

**2. Dr. M.V.P. Chandra Sekhara Rao** received his Ph.D. degree in Computer Science and Engineering from the Jawaharlal Nehru Technological University, Hyderabad. He is currently Professor in the Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, Andhra Pradesh, India. His research interests are Data Mining, Big Data Analytics and Privacy Preserving in Data Mining..

**REFERENCES**

1. A. F. Abate, G. L. Marcialis, N. Poh, and C. Sansone. **Introduction to the special issue on robustness, security and regulation aspects in current biometric systems (RSRA-BS),** *Pattern Recognition Letters*, Vol. 126, pp. 1–2, September 2019 doi: 10.1016/j.patrec.2019.07.004.
2. D. Akdoğan, D. KaraoğlanAltop, and A. Levi. **Secure key agreement based on ordered biometric features**, *Computer Networks*, Vol. 163, pp. 106885, November 2019, doi: 10.1016/j.comnet.2019.106885.
3. K. Atighehchi, L. Ghammam, M. Barbier, and C. Rosenberger. **GREYC-Hashing: Combining biometrics and secret for enhancing the security of protected templates**, Future Generation Computer Systems, Vol. 101, pp. 819–830, Dec. 2019 doi: 10.1016/j.future.2019.07.022.
4. F. S. Babamir and M. Kirci. **Dynamic digest based authentication for client–server systems using biometric verification**, Future Generation Computer Systems, Vol. 101, pp. 112–126, December 2019, doi: 10.1016/j.future.2019.05.025.
5. T. Bengs, **Putting authentication in the palm of your hand**, Biometric Technology Today, Vol. 2018, no. 7, pp. 8–11, July 2018 doi: 10.1016/S0969-4765(18)30095-X.
6. Babamir, F. and Kirci, M.. **Dynamic digest based authentication for client–server systems using biometric verification.** Future Generation Computer Systems, Vol. 101, pp.112-126, 2019.
7. P. Connor and A. Ross. **Biometric recognition by gait: A survey of modalities and features**, Computer Vision and Image Understanding, vol. 167, pp. 1–27, Feb. 2018, doi: 10.1016/j.cviu.2018.01.007.
8. L. Wang, B. Wang, W. Song, and Z. Zhang. **A key-sharing based secure deduplication scheme in cloud storage**, Information Sciences, Vol. 504, pp. 48–60, December 2019, doi: 10.1016/j.ins.2019.07.058.
9. S. Das. **Lip biometric template security framework using spatial steganography, Pattern Recognition Letters**, Vol. 126, pp. 102–110, September 2019 doi: 10.1016/j.patrec.2018.06.026.
10. Y. Cao, H. Ji, W. Zhang, and F. Xue,. **Visual tracking via dynamic weighting with pyramid-redetection based Siamese networks**, Journal of Visual Communication and Image Representation, Vol. 65, p. 102635, December 2019 doi: 10.1016/j.jvcir.2019.102635.
11. M. Gomez-Barrero and J. Galbally. **Reversing the irreversible: A survey on inverse biometrics,** Computers & Security, Vol. 90, p. 101700, Mar. 2020, doi: 10.1016/j.cose.2019.101700.
12. L. Fei, B. Zhang, W. Zhang, and S. Teng. **Local apparent and latent direction extraction for palmprint recognition**, Information Sciences, Vol. 473, pp. 59–72, January 2019 doi: 10.1016/j.ins.2018.09.032.
13. M. Gomez-Barrero and J. Galbally, **Reversing the irreversible: A survey on inverse biometrics**, Computers & Security, Vol. 90, p. 101700, March 2020, doi: 10.1016/j.cose.2019.101700.
14. W.-Y. Han and J.-C. Lee. **Palm vein recognition using adaptive Gabor filter, Expert Systems with Applications**, Vol. 39, no. 18, pp. 13225–13234, December 2012, doi: 10.1016/j.eswa.2012.05.079.
15. V. I. Ivanov and J. S. Baras, **Authentication of area fingerprint scanners,** Pattern Recognition, Vol. 94, pp. 230–249, October 2019 doi: 10.1016/j.patcog.2019.03.001.
16. N. Hu, H. Ma, and T. Zhan, **Finger vein biometric verification using Block Multi-scale Uniform Local Binary Pattern features and Block Two-Directional Two-Dimension Principal Component Analysis**, Optik, p. 163664, February 2020 doi: 10.1016/j.ijleo.2019.163664.
17. G. Jaswal, A. Kaul, and R. Nath, **Multiple feature fusion for unconstrained palm print authentication,** Computers & Electrical Engineering, Vol. 72, pp. 53–78, November 2018 doi: 10.1016/j.compeleceng.2018.09.006.
18. L. Shang, D.-S. Huang, J.-X. Du, and C.-H. Zheng, **Palmprint recognition using FastICA algorithm and**

**radial basis probabilistic neural network,** Neurocomputing, Vol. 69, no. 13, pp. 1782–1786, August 2006, doi: 10.1016/j.neucom.2005.11.004.

19. H. Kaur and P. Khanna/ **Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing,** Future Generation Computer Systems, Vol. 102, pp. 30–41, January 2020, doi: 10.1016/j.future.2019.07.023.
20. K. Ruth Ramya, M.V.P. Chandra Sekhara Rao,. **A Novel Fingerprint Minutiae based Authentication Framework for Cloud Services**, Journal of Theoretical and Applied Information Technology, Vol. 97(22), November 2019, PP 3209-3216.
21. K. Ruth Ramya, M.V.P. Chandra Sekhara Rao, **A novel multi-user fingerprint minutiae based encryption and integrity verification for cloud data**, International Journal of Advanced Computer Research, Vol. 8(37), July 2018, PP 161-*170.* https://doi.org/10.19101/IJACR.2018.837010
22. K. Ruth Ramya, Manjula Josephine B, Vara Prasad P, Manikanta B, Rithvik P, Sri Surya T,, **Pro Guard Malicious Social Network Account based Online Promotions**, International Journal of Emerging Trends in Engineering Research,, Vol. 8(4), 2020, PP 1319-1325. https://doi.org/10.30534/ijeter/2020/62842020
23. K. Ruth Ramya, Manjula Josephine B, Praveen K, Maruthi M, Kumar C, **An Efficient and Secured Biometric Authentication for IOT**, International Journal of Emerging Trends in Engineering Research,, Vol. 7(11), 2019, PP 604-609. https://doi.org/10.30534/ijeter/2019/327112019