Journal of Theoretical and Applied Information Technology
30th November 2019. Vol.97. No 22
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL FINGERPRINT MINUTIAE BASED AUTHENTICATION FRAMEWORK FOR CLOUD SERVICES

RUTH RAMYA KALANGI[1], Dr. M.V.P. CHANDRA SEKHARA RAO[2]

[1]Research Scholar, Acharya Nagarjuna University, Department of CSE, India

[2]Professor. RVR & JC College of Engineering, Department of CSE, India

E-mail: [1]ramya_cse@kluniversity.in, [2]manukondach@gmail.com

ABSTRACT

Biometric based Authentication plays a vital role for signature verification and user access control in the distributed cloud computing. Most of the traditional biometric based authentication models use single key for all cloud services authentication. Traditional biometric key based privacy preserving models depend on the static key generators for key extraction process. Limitations of traditional biometric based authentication models are number of keys, services and computational time. To resolve these issues, A Novel Fingerprint Minutiae based Authentication Framework for Cloud Data is proposed. This framework consists of fingerprint pattern extraction, integrity computation and authentication protocol for cloud service security. Experimental results are performed on Amazon AWS cloud services.

Keywords: *Fingerprint Minutiae Extraction, Cloud Services, Cloud Security, Biometrics, Hash, Authentication.*

1. INTRODUCTION

Due to large size datasets, data now-a-days is deployed in cloud. Confidentiality, Integrity and authentication are major aspects of security. Privacy of an user sensitive data & enterprise data is a major concern. Authentication is proving that the entity is the one it claims to be. Algorithms like Digital signature standard are used to prove authentication Existing Integrity algorithms include SHA, MD5 etc., Traditional attribute based encryption algorithms are based on user attributes Biometric techniques are considered to be reliable and secure when compared to traditional cryptographic approaches.

Integrity verification function is one of the essential cryptographic approaches used to integrate the hash value in the message authentication, digital signature and group communication. Cryptographic hash function takes a variable length data as input and generates a fixed length digest as output. Most of the traditional hash functions such as MD5, Whirlpool, SHA512 and chaotic hash maps are used to check the integrity of the text or file in the authentication protocols. Traditional integrity verification algorithms [2] are difficult to prevent attacks and collisions in static and dynamic cloud networks. Also, these algorithms are not very efficient for dynamic cloud networks for large size data. A large number of research works have been implemented on cryptographic integrity functions to authenticate data in the cloud computing. Authentication model is used to validate each client during the data communication.

Authentication is the process of verifying whether the user claiming cloud service or not in a remote cloud environment is authorized or not. It is also used to determine the security level of the cloud service on the authenticated user. Traditional authentication models [3][4] have been proposed in the literature to authenticate each cloud user for cloud services. Basically, these authentication models are time consuming and infeasible to authenticate large number of cloud services in remote cloud environment [5][6][7]. Zhendong [8] proposed a novel biokey generation algorithm to check the user authentication and biometric authentication to a single cloud service. The main problem in this model includes difficulty to handle multiple keys to each cloud service and integrity verification process.

In this paper, a novel fingerprint pattern based user authentication framework is implemented to verify the user authentication to cloud services. This framework is used to authenticate the cloud user and to initialize the cloud service in a secured way. In this model, multiple biokeys are used to validate user authentication in cloud environment. The main contributions proposed a new fingerprint feature extraction-based on integrity computation. Minutiae extracted from fingerprint patterns are also used to detect the integrity of the data stored in cloud. This work concentrates on a new multi-user authentication protocol that is designed and implemented on different cloud services for data security. One key feature of proposed protocol is instead of using a single key to access all the services of a single user different key are used to access different services of an user. Moreover CP-ABE algorithm which is considered to be an efficient algorithm for encrypting cloud data is used to send session key securely to the recipient.

2. RELATED WORK

Zhendong Wu et.al., [8], proposed FVHS, extracts strong bio-key sequences from finger-vein which combines It combines machine learning, biometrics, and cryptography technologies, Both a theoretical analysis and experimental verification show that FVHS can extract stable bio-keys from high quality finger vein images. FVHS can extract a finger vein bio-key with a Genuine Accept Rate of more than 99.9%, while the False Accept Rate is less than 0.8% and Rates less than 0.5%.

A. Cheng Chen, et.al. [9] in proposed FBF-DBN, nonlinear learning ability of deep neural network is used to recognize the features of finger veins. Improved deep network input by using feature points set in vein images sharply reduced the time in learning and detection, meeting the practical needs of biometric recognition specifically applied to embedded equipment. Experimental results showed that FBF-DBN algorithm presented better recognition performance and faster speed.

Salman Hammed Khan, et.al., [10] proposed a novel framework that applies random projections to biometric data (inherence factor), using secure keys derived from passwords (knowledge factor), to generate inherently secure, efficient and revocable/renewable biometric templates for users' verification. The results prove that the proposed framework does not undermine the discriminating features of genuine and forged signatures and the verification performance is comparable to that of the state-of-the-art benchmark results.

Jin Li, et.al [11]., proposed a Secure Outsourced ABE system, which not only supports secure outsourced decryption, but also provides secure outsourced key-issuing. Unlike the current outsourced ABE systems, our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the AAs and eligible users to perform locally.

Table 1: Comparison of Proposed Work to Existing Models.

L: Low; H: High; NA: Not Applicable

Metric	**ZhendongWu [8]**	**Cheng [9]**	**Salman [10]**	**Jin [11]**	**Proposed FMA Model**
Sensitivity on large data	L	M	M	M	H
Runtime (ms)	H	M	M	M	L
Multi-user with multi-cloud services	NA	NA	NA	NA	Applies
Dynamic hash size	No	No	No	No	Yes

3. PROPOSED MODEL

All existing models used extracted minutiae and used that extracted minutiae directly as session key and authenticator and only single key is used to authenticate all cloud services. This work mainly concentrates on the proposing an authentication protocol that uses minutiae extracted from fingerprint image. Minutiae thus extracted are given as input to hash algorithm that has high sensitivity and low computational time the output thus produced can not only used for integrity verification of minutiae extracted from user fingerprint but can also serve as key for encryption of session key that is distributed. The hash value thus generated also acts as an authenticator.In this proposed A Novel Fingerprint Minutiae based Authentication Model (FMA), fingerprint images are used to generate multiple bio keys. Mult-biokeys generated are used to authenticate cloud users. Proposed FMA Model is divided into three phases

i. Multi - biokey Extraction
ii. Hash value computation.
iii. Cloud User to Service Authentication.

As shown in figure 1, initially an optimized self-learning method is used to extract minutiae from the given fingerprint image using proposed Multi-biokey Extraction Algorithm (MBEA). These patterns are used as input to the multiple biokey generation process that generates multiple biokeys using proposed Adaptive Integrity Algorithm (AIA). Apart from generating multiple biokeys AIA algorithm is also used to generate hash or integrity value for the extracted fingerprint minutiae. Cloud User to Service Authentication using proposed Multi-biokey based User Authentication Process (MBUA).

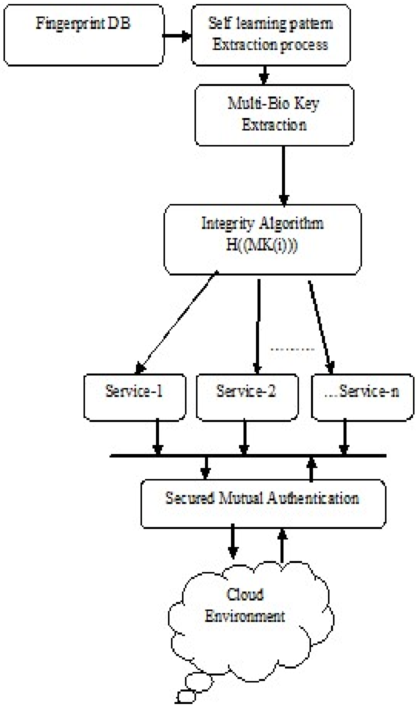

Fingerprint DB
Self learning pattern Extraction process
Multi-Bio Key Extraction
Integrity Algorithm H((MK(i)))
....
Service-1
Service-2
...Service-n
Secured Mutual Authentication
Cloud Environment

Figure 1: Fingerprint Minutiae based Authentication Model (FMA) Block Diagram

The basic notations used in the proposed framework are summarized in table 2.

Table 2: Notations used in Proposed FMA Model

Notation	Meaning
I(x,y)	Input Biometric Image
$\sigma^2_{I(x,y)}$	Variance
W	Image Width
H	Image Height
$N(x,y)$	Normalized Image
α_1 and α_2	140 -150
ρ_0 and ρ_1	250-255
$N_{min}(x,y)$	Minimum value in Normalized block data
$N_{max}(x,y)$	Maximum value in Normalized block data
T_X	X pixel value in Transformed image T.
T_Y	Y pixel value in Transformed image T.
r	Gaussian Random value
$D_{x_c}(x_c, y_c)$	Derivative w.r.t x
P 1	Derivative w.r.t y
$\theta(x_c, y_c)$	Angle of curvature
S	Filtered Image
R(x,y)	Minimum Oriented Curve of Fingerprint Pattern
T(x,y)	Transformed Image
CP(x,y)	Curvature of Fingerprint Pattern

3.1 Multi-biokey Extraction Algorithm (MBEA)

Minutiae are extracted from fingerprint using Multi-biokey Extraction using Multi-biokey Extraction Algorithm (MBEA). This algorithm takes fingerprint image as input and produces

Minutiae as output.. This algorithm has less computational time when compared to existing algorithms. Input to algorithm 1 is Fingerprint Image I(x,y) and output produced is Multi-biokeys.

Algorithm 1 Multi-Biokey Extraction Algorithm (MBEA)

Step1. Read input image I(x,y) =Fingerprint (i);
Step2. Pre-processing the input image I(x,y) using the normalization measure
Step3. Transform the normalized image.
Step4. Apply the self-learning manifold filter using the objective function.
Step5. Find the fingerprint pattern orientation curves using the orientation of the self-learning manifold filter.
Step6. The binary code patterns of each block in the 8x8 size window are stored in BP[]..
Step7. For each binary pattern Bi in BP [] generate biokey BK[] using Adaptive Integrity

---

In step 1 fingerprint image is taken as input In step 2 pre-processing is done on input fingerprint image using equation 1

$$I_N(x,y)=\frac{1}{|W||H|}\sum_{i=0}\sum_{j=0}I(x,y)$$

$$\sigma^2_{I(x,y)}=\frac{1}{|W||H|}\sum_{i=0}^{|W-1}\sum_{j=0}^{|H-1}(I(x,y)-I_N(x,y))^2$$

$$N(x,y)=\alpha_1+\frac{\sqrt{\rho_0}}{\sigma_{I(x,y)}}(I(x,y)-I_N(x,y));\text{if } I(x,y)>=I_N(x,y)$$

$$N(x,y)=\alpha_2-\frac{\sqrt{\rho_1}}{\sigma_{I(x,y)}}(I(x,y)-I_N(x,y));\text{if } I(x,y)<I_N(x,y)\quad\text{—(1)}$$

Where α_1 and α_2 are the initial random mean values taken from the range 140 to 150. Here, α_1 and α_2 are fixed due to the mean value of block pixel intensity of input image varies between 140 to 150. Variables ρ_0 and ρ_1 are the initial random variance values taken from the range 250 to 255. Similarly, ρ_0 and ρ_1 are fixed due to the variance value of block pixel intensity of input image varies between 140 to 150. After the image normalization process, the output image $N(x,y)$ is given to the image transformation step 3 As described in Step 4 apply the self-learning manifold filter using the following objective function as shown in equation 2.

$$T(x,y)=\text{round}\left(\frac{N(x,y)-N_{min}(x,y)}{N(x,y)-N_{max}(x,y)}.\text{Scalefactor}\right)$$

Where Scale factor=(Max-0)=(255-0)=255

$$S(x,y)=\frac{1}{2\pi\sigma_X\sigma_Y}\exp\left(-0.5\left(\frac{T_X^2}{\sigma_X^2}+\frac{T_Y^2}{\sigma_Y^2}\right)\text{cosine}(2\pi r\,T_x)\right)\quad\text{----(2)}$$

In step 5 find the fingerprint pattern orientation curves using the orientation of the self-learning manifold filter as shown in equation 3.

$$R_{x_c}(x_c,y_c)=\sum_i\sum_j 2.D_{x_c}(x_c,y_c).D_y(x_c,y_c)$$

$$R_{y_c}(x_c,y_c)=\sum_i\sum_j 2.D_{y_c}(x_c,y_c).D_y(x_c,y_c)$$

$$\theta(x_c,y_c)=\frac{1}{2}\tan^{-1}\left(r.\frac{R_{x_c}(x_c,y_c)}{R_{x_c}(x_c,y_c)}\right)\quad\text{-----(3)}$$

$r\in$ Gaussian Random Value

The minimum oriented curve of the fingerprint pattern is obtained by using the second derivative of the filtered image S as shown in equation 4.

$$CP(x,y)=\frac{\partial^2 S}{\partial x_c^{\,2}}\cos^2\theta(x_c,y_c)+2.\frac{\partial^2 S}{\partial x_c\partial y_c}\cos\theta(x_c,y_c).\sin\theta(x_c,y_c)$$
$$+\frac{\partial^2 S}{\partial y_c^{\,2}}\sin^2\theta(x_c,y_c)$$

$$CP(x,y)=\begin{pmatrix}\cos\theta(x_c,y_c) & \sin\theta(x_c,y_c)\end{pmatrix}\begin{bmatrix}\frac{\partial^2 S}{\partial x_c^{\,2}} & \frac{\partial^2 S}{\partial x_c\partial y_c}\\ \frac{\partial^2 S}{\partial y_c\partial x_c} & \frac{\partial^2 S}{\partial y_c^{\,2}}\end{bmatrix}\begin{pmatrix}\cos\theta(x_c,y_c)\\ \sin\theta(x_c,y_c)\end{pmatrix}\quad\text{—(4)}$$

Here the hessian matrix is used to compute the Eigen values for the minimum and maximum curvature points in the fingerprint image as shown in equation 5.

$$HM=\begin{bmatrix}\frac{\partial^2 S}{\partial x_c^{\,2}} & \frac{\partial^2 S}{\partial x_c\partial y_c}\\ \frac{\partial^2 S}{\partial y_c\partial x_c} & \frac{\partial^2 S}{\partial y_c^{\,2}}\end{bmatrix}\quad(5)$$

Let λ^1 and λ^2 represents the Eigen values obtained by solving HM matrix.

The maximum curve detected in the fingerprint is given by max $\{\lambda^1, \lambda^2\}$ and the minimum curvature detected in the fingerprint central point of the block size window is given by min $\{\lambda^1, \lambda^2\}$. Finally, local binary pattern is applied on the resultant image to find the binary pattern of the fingerprint. A local binary pattern in the fingerprint pattern is used to find the ordered set of binary information by using the central pixel with its neighbour pixels. The LBP of processed image S is given by equation 6.

$$\mathrm{LBP}\left(S\left(x_c, y_c\right)\right) = \sum_{i=0}^{7} f(S(x_i) - S(x)_c).2^n \qquad \text{---(6)}$$

where f(m)=1 if m>=0

else f(m)=0 if m<0

Here, binary code of each block in the LBP operator is extracted in clockwise direction from top left. The binary code patterns of each block in the 8x8 size window are stored in BP [] as described in step 6. Using Adaptive Integrity Algorithm described in in section 3.2 generate biokey BK [] for each binary pattern B_i in BP [].

3.2 Hash Value Computation Using Adaptive Integrity Algorithm (AIA)

Initially, each cloud service details and bio-key generated from fingerprint pattern are taken as input Adaptive Integrity Algorithm (AIA) is described in algorithm 2. Here, input message M is partitioned into blocks and then sub-blocks of size 32-bits each. If the size of the input message exceeds its hash size then the message is padded with '1' followed by zeros. For each sub-block partition performs a set of polynomial transformations to find the hash value. AIA is the novel solution to the integrity verification in cloud computing environment. Finally, AIA algorithm is efficient in terms of high sensitivity, less time and memory. L. Zhou r et.al. [1], a novel integrity computation algorithm is designed and implemented to check the data security in the cloud computing. In this paper, the block processing operation proposed in Zhou r et.al. [1] is optimized to improve the data sensitivity and randomization. Input to AIA algorithm is Minutiae extracted from fingerprint Image and output produced out of this algorithm is Hash values that serve as Mufti-biokeys.

Algorithm 2. Adaptive Integrity Algorithm (AIA)

```
Step 1. For each block partition in P[i]
Step 2. For each round r in #R
Step 3. Q and R are vectors obtained by solving QR decomposition formula on input data partition.
Step 4. Compute T1, T2 and T3.
Step 5. Compute H[i] by concatenating T1, T2, T3.
Step 6. Repeat step 1 to step 5 until all blocks of p[] are processed.
```

In step 1 Minutiae extracted from fingerprint are stored in an array P[i]. Step 2 describes number of rounds. Number of rounds is of user choice. Q and R are vectors obtained by solving QR decomposition formula on input data partition. Here, QR decomposition formula is used to find the Q and R vectors. QR=[b1,b2…..br]=P[i] in step 3. Compute T1, T2, T3 as described using the following equations in step 4. As stated in step 4 compute H[i] by concatenating T1, T2 and T3. Repeat step 1 to step 5 until all blocks of p[] are processed as shown in equation 7.

$$T_1 = SK^T.[Q.\psi\left(SK\right).\ \mathrm{CauchyLB}\left(\mathrm{Poly}\left(SK\right)\right]$$

$$T_2 = \left(\frac{[Q.\psi\left(SK\right).\ \mathrm{CauchyUB}\left(\mathrm{Poly}\left(SK\right)\right]}{\log(\sum SK[i])}\right)$$

$$T_3 = \left\lfloor T_1 \mathrm{scale}(256) \right\rfloor \qquad (7)$$

Table 3 represents all the notations used in AIA algorithm.

Table 3: Notations used in AIA Algorithm

Notation	Meaning
SK	Random Secret key
P[i]	Input blocks partition data.
$\psi(SK)$	Rank of the input secret key SK.
Cauchy LB	Cauchy lower bound to the polynomial equation of SK.
Cauchy UB	:Cauchy upper bound to the polynomial equation of SK
T_1, T_2, T_3	Three temporary variables.
#NR	Number of rounds

H[i]	Round hash value
H	Final Hash value.

3.3 Cloud User to Service Authentication

Users are authenticated to cloud services using Multi-biokey based User Authentication Process (MBUA), each user is authenticated using the user's bio-key and its hash value for secure data exchange as shown in figure 2.

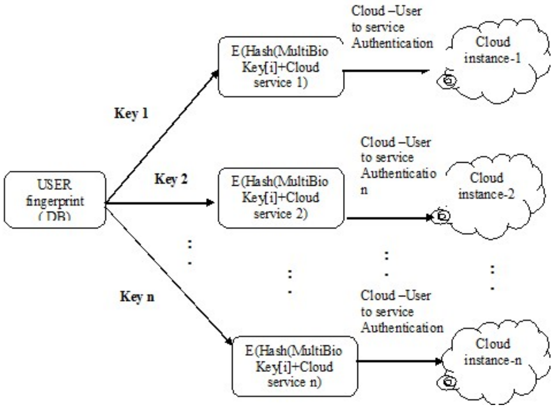

USER
fingerprint
(DB)
Key 1
Key 2
Key n
E(Hash(MultiBio Key[i]+Cloud service 1)
E(Hash(MultiBio Key[i]+Cloud service 2)
E(Hash(MultiBio Key[i]+Cloud service n)
Cloud –User to service Authentication
Cloud –User to service Authenticatio n
Cloud –User to service Authentication
Cloud instance-1
Cloud instance-2
Cloud instance-n

Figure 2: Multi-biokey based User Authentication Process (MBUA)

According t0 step 1 in the proposed MBUA algorithm, user's multiple-bio-key binary patterns is generated and initialized at the cloud user side as MK_i. Next as per step 2, a chaotic Gaussian random number is selected G_k. Later in step 3, hash value is computed on the multiple-bio key and Gaussian random number. Here, the computed hash value is encrypted using the traditional ciphertext policy attribute based encryption (CP-ABE) approach for authentication using the equation 8.

$$MH_i = Enc(Hash(MK_j \mid G_k), Mk_j) \quad (8)$$

Step 4, encrypts hash value is used as shared key MH_i between the user and cloud service provider for cloud service URL access (Cloud service URL-1),In the step 5, hash value of the cloud service URL is encrypted. This encrypted hash value, shared bio-key and random nonce are sent to cloud user for session key initialization using equation 9.

$$Enc(Hash(CloudserviceUrl\_1|), MK_j) \mid MH_i \mid Nonce_1 \quad (9)$$

In the step 6, cloud user decrypts the hash value using the shared bio-key. This decrypted cloud service URL and MH_i are used to form a session key to each requested cloud service.

$$SessionKey\_CS1 = Dec(Hash(CloudserviceUrl\_1|), MK_j) \mid MH_i \quad (10)$$

Step 7 Finally, session key and random nonce $SessionKey\_CS1 \mid Nonce1$ are verified at the cloud server for user authentication as shown in algorithm 3. This process repeats for rest of the cloud services. Input to MBUA algorithm is Multi-biokeys and output is Session Key.

Algorithm3. Multi-biokey based User Authentication (MBUA).

Step1. User generates Multi-biokeys using the fingerprint patterns as MK_i

Step2. User generates Gaussian Random number as G_k

Step3. User Generates MH_i that acts as authenticator.

Step 4. User transmits Authenticator MH_i and cloud service URL

Step 5. Server sends session key to user

Step6. Session key sent by the server is decrypted by the user

Step7. User sends session key & nonce to server

----

4. EXPERIMENTAL RESULTS

Results are analyzed using real-time Amazon AWS cloud server on different types of services. In the Amazon AWS environment, different types of services are initiated to each user for secured authentication process. Here, different variables or parameters such as data size, sensitivity, runtime, and user policies are used to verify the efficiency of the proposed model compared to the existing models Proposed FMA model is implemented in three phases, in the initial phase, user's fingerprint are used to compute the multiple-bio keys using (MBEA). These multiple-biokeys are given to hash algorithm (AIA) to find the integrity of the patterns for user to cloud authentication process. In the third phase, user authentication process is performed to each cloud service in order to initialize the session key for cloud service usage using (MBUA).

Let B (1), B(2),….B(k) are the change in bits in integrity values as shown in equation 11.

$$\text{Sensitivity in bit rate } S = \sum_{i=1}^{n} B(i)/N \quad (11)$$

Where N means size of the integrity value.

Figure 3 illustrate the sample fingerprint input image of cloud user. Figure 4 Fingerprint image after Image enhancement. Enhanced is Thinned. For Thinning we use Library. From Thinned image minutiae are extracted using proposed MBEA algorithm.

Figure 3: Sample Input Fingerprint Image

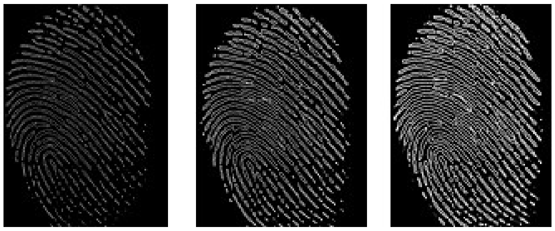


Figure 4: (a)Fingerprint Image After Image Enhancement, (b) Fingerprint Image After Thinning, (c) Minutiae Extraction from Fingerprint.

Table 4 describes the computational time of fingerprint pattern extraction process on training fingerprint images. The average runtime of the proposed MBEA algorithm is less than the traditional approaches such as LBP, SIFT and manifold learning on different data sizes.

Table 4: Average Computational Time of Fingerprint Extraction Methods on Fingerprint Samples of Various Sizes

DB Size	LBP (ms)	SIFT (ms)	Manifold learning (ms)	MBEA (ms)
10	984.98	835.23	814.79	793.43
25	1035.35	963.13	924.63	910.19
50	1058.24	983.53	936.35	920.64
100	1182.53	1007.35	979.16	947.25

Figure 5 describes the computational time of fingerprint pattern extraction process on training fingerprint images. The average runtime of the proposed MBEA algorithm is less than the traditional approaches such as LBP,SIFT and manifold learning on different data sizes

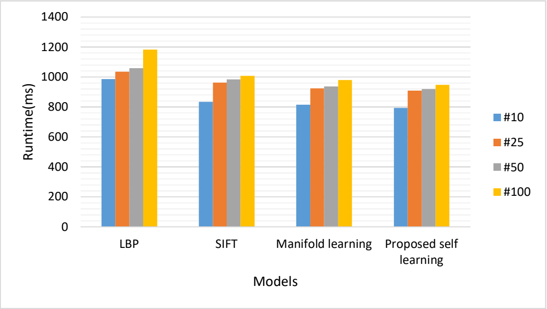
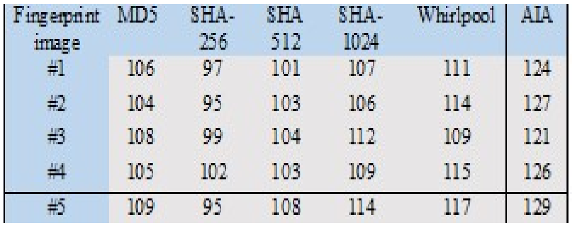


Figure 5: Average Computational Time of Fingerprint Extraction Methods on Fingerprint Samples.

Table 5, illustrates the comparative analysis of proposed AIA algorithm hash approach to the existing hash approaches on sensitivity. From the table, it is noted that the proposed AIA hash method has high sensitivity than the traditional methods on different fingerprint images.

Table 5: Comparison of Sensitivity of Various Hash Algorithms with AIA Algorithms.

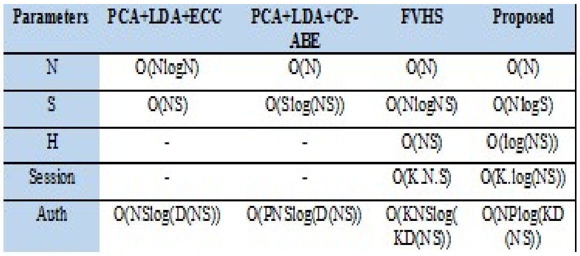


Fingerprint image	MD5	SHA-256	SHA 512	SHA-1024	Whirlpool	AIA
#1	106	97	101	107	111	124
#2	104	95	103	106	114	127
#3	108	99	104	112	109	121
#4	105	102	103	109	115	126
#5	109	95	108	114	117	129

In the table 6, the complexity of the various parameters such as number of users, number of cloud services, Hash sensitivity, session key generation and overall authentication process are summarized. From the table, the complexity of the proposed framework is less compared to the traditional approaches on different parameters.

Table 6: Complexity analysis of User to Cloud Service Authentication Process.

N: Number of user, S: Number of cloud services , H: Hash function , Session :Session key, Auth: Authentication , K: Biokey, P:Policies, D: Data



Parameters	PCA+LDA+ECC	PCA+LDA+CP-ABE	FVHS	Proposed
N	O(NlogN)	O(N)	O(N)	O(N)
S	O(NS)	O(Slog(NS))	O(NlogNS)	O(NlogS)
H	-	-	O(NS)	O(log(NS))
Session	-	-	O(K.N.S)	O(K.log(NS))
Auth	O(NSlog(D(NS))	O(PNSlog(D(NS))	O(KNSlog(KD(NS))	O(NPlog(KD(NS))

5. CONCLUSION

FMA model is used to validate or check user level security towards the cloud services. This model is implemented on cloud data to enhance security against third party attacks. Multiple biokeys are generated from minutiae extracted from fingerprint of users so that an user can use different biokey for each service authentication. Hash algorithm AIA is applied on the extracted minutiae to preserve integrity and to transfer authenticator securely. Experimental results on various sizes of data shows that FMA model has less computational time, High efficiency, Sensitiveness and accuracy when compared to traditional cloud security models.

REFRENCES:

[1] L. Zhou, X. Li, K. Yeh, C. Su and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance", Future Generation Computer Systems, vol. 91, pp. 244-251,2019.

[2] Jiawei Yuan and Shucheng Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification", IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, 2015. Available: 10.1109/tifs.2015.2423264

[3] V. Kumar, M. Ahmad and A. Kumari, "A secure 2019. Available: 10.1016/j.tele.2018.09. elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS", Telematics and Informatics, vol. 38, pp. 100-117, [Accessed 10 April 2019].

[4] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun and K. Sakurai, "Authentication in mobile cloud computing: A survey", Journal of Network and Computer Applications, vol. 61, pp. 59-80, 2016.

[5] I. I., R. P.M. and V. Bhaskar, "Encrypted token based authentication with adapted SAML technology for cloud web services", Journal of Network and Computer Applications, vol. 99, 2017, pp. 131-145.

[6] C. Li, D. Shih and C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems", Computer Methods and Programs in Biomedicine, vol. 157, pp. 191-203, 2018.

[7] H. Jannati and B. Bahrak, "An improved authentication protocol for distributed mobile cloud computing services", International Journal of Critical Infrastructure Protection, vol. 19, 2017,pp. 59-67, 2017.

[8] Wu, Zhendong & Longwei, Tian & Li, Ping & Wu, Ting & Jiang, Ming & Wu, Chunming. “Generating Stable Biometric Keys for Flexible Cloud Computing Authentication using Finger Vein. Information Sciences”. 2016, 433-434.

[9] Cheng Chen, Zhendong Wu, Ping Li, Jianwu Zhang (2015), inger Vein Recognition Algorithm Using Feature Block Fusion and Depth Neural Network, ok Computational Intelligence and Intelligent Systems: 7th International Symposium, ISICA 2015, Guangzhou, China, November 21-22, 2015, Revised Selected Papers, pp.572-583.

[10] Salman Hameed Khan, Muhammad Ali Akbar,Farrukh Shahzad, Mudassar Farooq. (2014). Secure biometrc template generation for Multi-Factor authentication, Pattern Recognition 48(2) · September 2014 *with* 238 Reads DOI: 10.1016/j.patcog.2014.08.024.

[11] Salman Hameed Khan, Muhammad Ali Akbar,Farrukh Shahzad, Mudassar Farooq. (2014). Secure biometrc template generation for Multi-Factor authentication, Pattern Recognition 48(2) · September 2014 *with* 238 Reads DOI: 10.1016/j.patcog.2014.08.024.

[12] B.Tirapathi Reddy,Dr.M.V.P.Chandra Sekhara Rao, Performance evaluation of various data deduplication schemes in cloud storage, IJPAM, Vol. 116, Issue No.5, 2016, pp. 175-180.

[13] B.Tirapathi Reddy,Dr.M.V.P. Chandra Sekhara Rao, “Data deduplication in cloud storage using dynamic perfect hash functions” ,Journal of Advanced Research in Dynamical and Control Systems, Vol.9,Sp Issue 12, 2017, pp. 2121-2132,