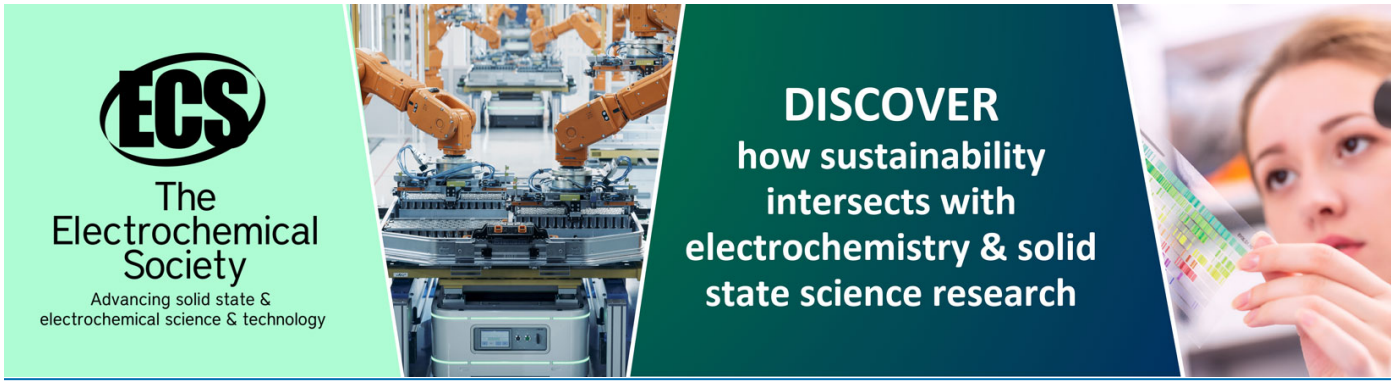
A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing



IOP Conf. Series: Materials Science and Engineering **981** (2020) 022043 doi:10.1088/1757-899X/981/2/022043

A Coherent and Privacy- Protecting Biometric Authentication Strategy in Cloud Computing

Bonthala Prabhanjan Yadav[1], Ch. Shiva Sai Prasad[2], Ch Padmaja[3], Seena Naik Korra[4], Sudarshan E[5]

[1,2,3,5]Sumathi Reddy Institute of Technology for Women, Warangal, India.
[4]SR Engineering College, Warangal, India.

[1]prabhanjanyadav2020@gmail.com

Abstract: The Biometric authentication has become progressively more desired in current years. With this expansion of cloud computing, database holders be influenced to expand this extensive volume of biometric information & detection operations to CLOUD for eradicate of this high-priced storage and result overheads, is still conveys possible dangers to users' seclusion. In this document, we recommend an well-organized, well planned and confidentiality-protecting biometric classification strategy. Particularly, biometric information was encrypted & farmed out for Cloud database. For complete a biometric confirmation, server holder encrypts the inquiry information and proposes that to cloud. The Cloud implements recognition tasks on the encrypted server and sends this conclusion to the server holder. The systematic protection assessment specifies the recommended system is protected still if attackers can fake detection appeals and conspire through the cloud. Evaluated with previous protocols, investigational and new outcomes prove the recommended strategy accomplishes enhanced performance in both preparation and discovery measures.

1. Introduction

Biometric identification has elevated progressively recognition by reason of it gives a optimistic approach to authenticate users. Compared with ordinary identification procedures established on keys and identification licenses, biometric authentication be examined to be additional genuine and suitable [1]. Moreover, biometric verification have be unanimously useful in various areas by utilizing biometric features are, iris [3], fingerprint [2] and facial patterns [4], which are accumulated as of various sensors [5-10].

For this biometric verification representation, record holder for instance the FBI who is in charge for administrate the nationwide biometric server, may desire to subcontract vast biometric information for Cloud database (e.g., amazon) to do away with an exorbitant storage and working out prices. Although, for defend the confidentiality of biometric data, this biometric information is changed to encryption information before externalizing. On any occasion a FBI's associate (e.g., PoliceStation) need for verify person's validation, that person changes to FBI & creates an validation inquiry with helping the person's biometric distinctiveness (e.g., VoicePatterns, Irises, FingerPrints, FacialPatterns etc.). In addition, the FBI converts request will be given to cloud to find out the well matched. Therefore, this difficult issue was how to implement procedure warrants the coherent and confidentiality- protecting Biometric authentication strategy in the Cloud Computing.

The group of confidentiality-protecting Biometric verification results has projected. But, majority of these mostly focused on confidentiality protection except disregard the coherence, they are the strategies found on Homomorphic encryption & unaware transference in to face image & Fngerprint authentication correspondingly. Facing starting rendition difficulties of restricted devices, these strategies will never coherent if this capacity of the server is more than Ten megabytes. After that, Evans [12] introduced a biometric authentication policy by using cipher text packing & circuit design methods to attain well-organized authentication to a large information storage space up to 1gb. In addition, Yuan and Yu [13] introduced a well-organized confidentiality preserving biometric identification method. Especially, they designed 3 elements and implemented a specific procedure to achieve the security of biometric feature. For enhancing the effectiveness, in this strategy, the server holder gives authentication matching operations to the cloud. Although, Zhuetal pointed out that Yuanandyu's procedure could also smashed with a complicity attack introduced with a malevolent client and cloud. Wang [14] launched a strategy cloud bi-ii is utilized unsystematic diagonal matrices to accomplish biometric validation. Though, this scheme is proved unprotected in [15], [16].

In this document, we recommend a coherent and confidentiality- protecting biometric authentication strategy in the cloud computing. Which can hold out against the collusion attack introduced by the cloud and the users. Especially, the core endowment will summarize below:

i. We investigate the biometric authentication strategy & show its inadequacies & security fragility in the introduced level-three violence. Specifically, it illustrate, hacker will retrieve these SecretKeys by collaborating to Cloud&then decrypt this Biometric characteristics for all customers.
ii. We introduce new coherent & privacy- protecting Biometric authentication strategy. Comprehensive protection examination explains that the introduced strategy will attain the required level for confidentiality Protection. Especially, this strategy is protected in the Biometric authentication Out Sourcing representation & will also go beside the attack introduced by.
iii. Evaluated for this old biometric verification strategies, the performance examination gives the introduced strategy gives a less computational price value in both research and authentication models.

2. Models And Designgoals

This part presents the system model, attack model, design goals.

2.1 Systemmodel

According to Fig, 3 special kinds of entities are there in this system along with the server holder, clients and the cloud. The server holder stores huge amount of biometric information (i.e., irises, fingerprints, facial patterns and voice etc.), and the biometric information is converted & sent for the CLOUD to storage. If a client asks to recognize himself/herself, a inquiry appeal was transferred to the server holder. Behind getting the appeal, the server holder creates encrypted cipher text to the biometric attribute and then sends encrypted cipher text for cloud for verification[10]-[12]. The server discovers the top and near equivalent to the encrypted inquiry call & transfers associated indicator for database holder. At the end, the database owner checks the comparability betweenthe encrypted query request and the biometric information corresponding to the index, sends the query outcome to the client.

2.2 Attackmodel

First, the Cloud DataBase was treated to be "honest but curious". The cloud powerfully goes after this developed and the implemented protocol, however gives attempts to disclose confidentiality from the database holder and the client[17][18][19]. An attacker will notice entire information which is kept in the cloud along with the encrypted biometric information, encrypted query requests & also the

corresponding consequences. The attacker will behave like a client to create query requests.
So, we divided the attack representation into the 3 levels as show below:

i. *Level I* : Attackers will just monitor the encrypted information which is located in cloud server. It is the well-known cipher text-only attack method.

ii. *Level II* : Moreover, encrypted information which is stored in cloud server, attackers can capable to obtain few of biometric attributes in the folder *D* although they don't recognize the respective encrypted cipher texts of record *C* , it is same for the known-candidate attack method.

iii. *Level III* : Attackers in this level will be applicable authenticated clients. So, attackers will create duplicate lots of recognition query requests as likely and gets the equivalent encrypted cipher texts. It is known-plaintext attack method.

A Biometric verification policy was safe if that will hold against the all 3 level-attacks. If the recommend approach will stop level-II and level-III attacks, this is never representing that attacker will a genuine client and notice few plaintexts from the biometric database. It is a very strong type of attack & no models are implemented to work in opposition to this type of attack [14].In this document, we concentrate happening to combined attack among a malevolent client & the cloud server. We introduce the connection among the encrypted cipher texts and the plaintexts of the biometric database, which is never recognized by the attacker, and it was extremely related to the attack method.

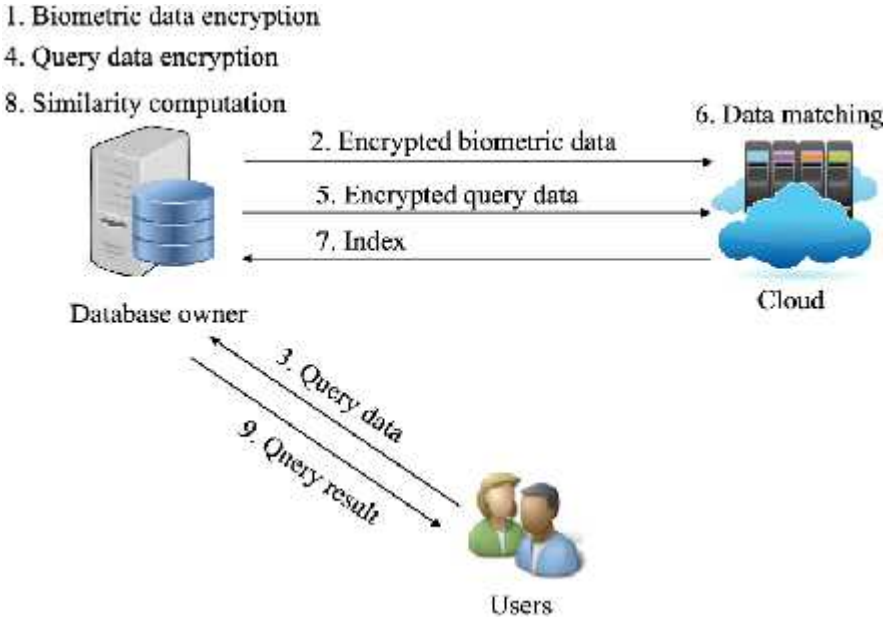


Fig 1. System model.

2.3 Designgoals

For getting, both protection and effectiveness, we presented in the new introduced strategy. The implementing objectives of the proposed method are:

i. *Efficiency*: Computational prices must be to be as less as likely at server owner side & the client side. For achieving more efficiency, all biometric identification jobs must be processed in the cloud.

ii. *Protection*: In the recognition model, the confidentiality of biometric information must be confined. Attackers & the semi-honest cloud must study not anything regarding the responsive information.

3. Performance Analysis

For assessing this execution of newly introduced design, we implement a cloud-related confidentiality-protecting finger print verification Scheme . To the cloud, we have 2 number of nodes with Intel6-core Xeous CPU 2.10 GHzand memory -32GB. We use a laptop with an2.40 GHz Intel Core CPU and memory-8GB, the inquiry request Finger Codes are indiscriminately choosen as of the database server that contains the Random640EntryVectors.

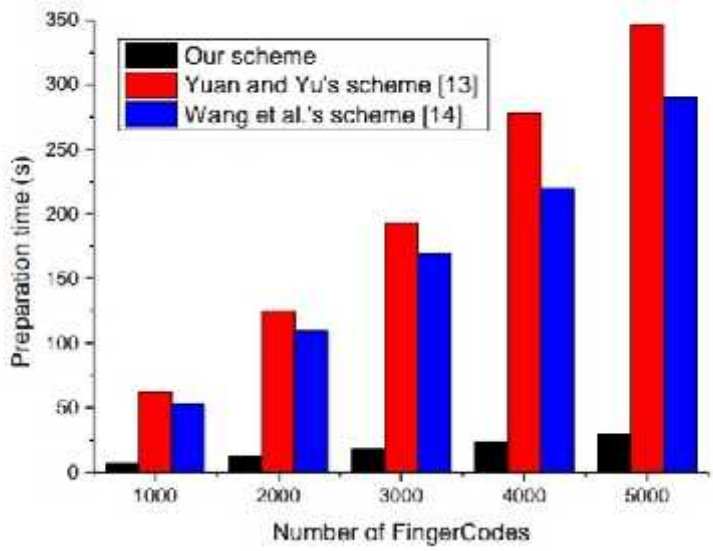


Fig 2. Time costs in the preparation phase.

TABLE 2. A summary of complexity costs. In the table, n denotes the number of FingerCodes in the biometric database of the

		Phases	Yuan and Yu's scheme [13]	Wang et al.'s scheme [14]	Our scheme
Computation	Database owner	Preparation	$O(nm^2)$	$O(nn^2)$	$O(nn^2)$
		Identification	$O(n^2)$	$O(n^2)$	$O(n^2)$
		Retrieval	$O(n)$	$O(n)$	$O(n)$
	Cloud server	Identification	$O(nn^2+n\log n)$	$O(nn^2+n\log n)$	$O(nn^2+n\log n)$
Communication	User	Identification	/	/	/
		Preparation	$O(nn^2)$	$O(nn^2)$	$O(nn)$
	Database owner	Identification	$O(n^2)$	$O(n^2)$	$O(n^2)$
		Retrieval	$O(1)$	$O(1)$	$O(1)$
	Cloud server	Identification	/	/	/
		Retrieval	$O(1)$	$O(1)$	$O(1)$
	User	Identification	$O(1)$	$O(1)$	$O(1)$

3.1 Complexity Analysis

Above table gives working out and communication Prices of the information holder side, clients and cloud server in our policy &the schemes in [13,14]. Each Matrix Multiplication costs O(n3), and n represents the Size for this Finger Code, and the categorization price of blurry Euclidean spaces have TimeComplexity of O(mlogm). As Demonstrated on the above table, here the new strategy has fewer complexities in the research stage. Here, mostly the computation and bandwidth expenses are decreased for database owner. In verification stage, the computation complexity for new policy was

very less than that in [14]. This motivation for this new Procedure executes vector-matrix multiplication tasks to searches for close near equivalent, while requires for perform MatrixMultiplication tasks. Though the complexity of this new strategy is similar as in [13], we focous on the [13] Sacrifices the considerable protection for attain such quickly and speed Computations for Pi. Moreover, this new strategy performs smaller amount of multiplication tasks [20-22], then gives good performance.

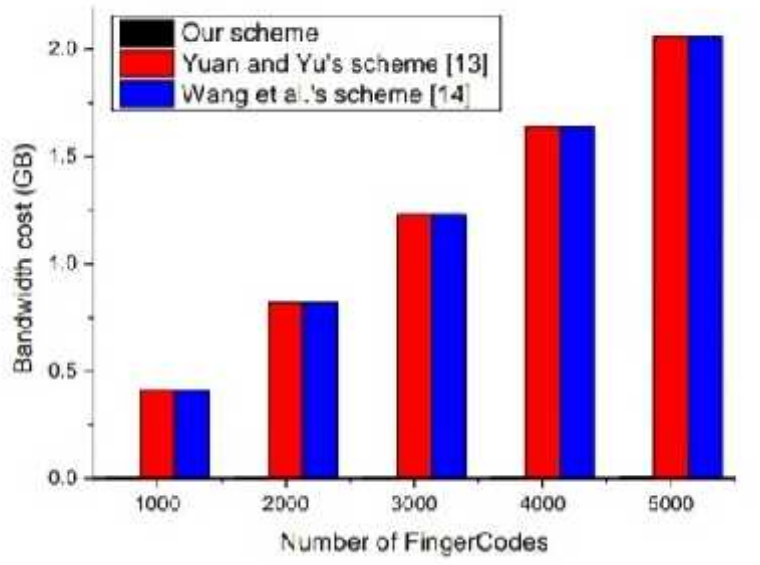


Fig 3. Bandwidth costs in the preparation phase.

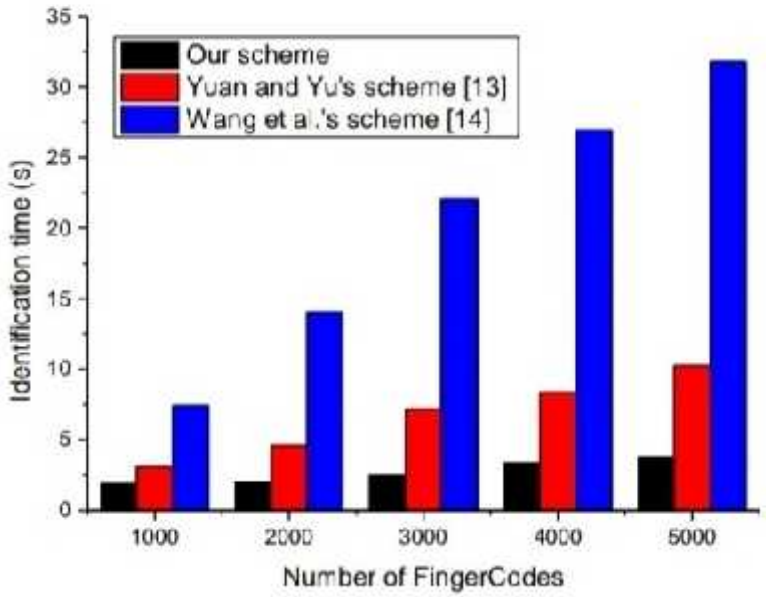


Fig 4. TimeCosts on identification time

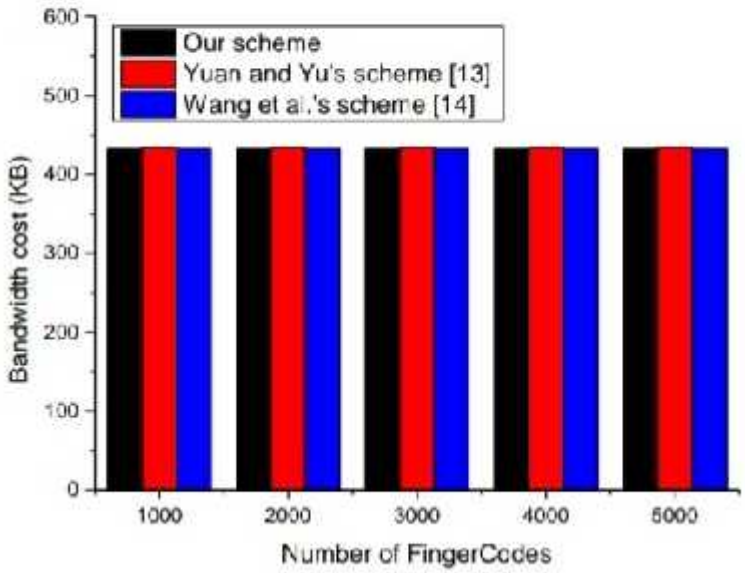


Fig 5. BandwidthCosts on identification phase.

4. Conclusion

In this document, we implemented a latest privacy-protecting Biometric Authentication strategy for the cloud computing. For Understand the good organization and safe requirements, we introduced a novel encryption procedure and cloud verification Guarantee. Performance assessments, of this introduced system meets the effectiveness require well.

5. References

[1] R Allen, P Sankar and S Prabhakar, “Fingerprint identification technology,” Biometric Systems, pp 22-61 2005
[2] A Jain, L Hong and S Pankanti, “Biometric identification,” Communications of the ACM, vol 43 no 2 pp 90-98 2000
[3] J de Mira, H Neto, E Neves, et al, “Biometric-oriented Iris Identification Based on Mathematical Morphology,” Journal of Signal Processing Systems, vol 80 no 2 pp 181-195 2015
[4] Sunil, G, Aluvala, S, Yamsani, N, Chythanya, KR &Yalabaka, S 2019, "Security enhancement of genome sequence data in health care cloud", International Journal of Advanced Trends in Computer Science and Engineering, vol 8 no 2 pp 328-332
[5] Y Xiao, V Rayi, B Sun, X Du, F Hu, and M Galloway, “A survey of key management schemes in wireless sensor networks,” Journal of Computer Communications, vol 30 no 11-12 pp 2314-2341 2007
[6] Sheshikala, M, Mohmmad, S & Shabana 2018, "Survey on multi level security for IoT network in cloud and data centers", Journal of Advanced Research in Dynamical and Control Systems, vol 10 no 10 Special Issue pp 134-146
[7] S Romdhani, V Blanz and T Vetter, “Face identification by fitting a 3d morphable model using linear shape and texture error functions,” in European Conference on Computer Vision, pp 3-19 2002
[8] Sampath Kumar, T, Manjula, B & Srinivas, D 2017, "A new technique to secure data over cloud", Journal of Advanced Research in Dynamical and Control Systems, vol 2017 no Special Issue 11 pp 391-396
[9] X Du, Y Xiao, M Guizani, and H H Chen, “An effective key management scheme for

heterogeneous sensor networks," Ad Hoc Networks, vol 5 no1 pp 24-34 2007
[10] Sai Keerthana, K, Harshavardhan, A & Ramesh, D 2019, "A privacy-preserving protocol for verifiable file search on the cloud", International Journal of Innovative Technology and Exploring Engineering, vol 8 no 6 Special Issue 4pp 476-479
[11] X Hei, and X Du, "Biometric-based two-level secure access control for implantable medical devices during emergency," in Proc of IEEE INFOCOM 2011 pp 346-350 2011
[12] Mounika, S & Sampath Kumar, T 2019, "Client –requirement fulfil QOS in multi server for max beneficial in cloud computing", International Journal of Advanced Science and Technology, vol 28 no 7 pp 44-49
[13] J Yuan and S Yu, "Efficient privacy-preserving biometric identification in cloud computing," in Proc of IEEE INFOCOM 2013, pp 2652-2660 2013
[14] QWang, S Hu, K Ren, et al, "CloudBI: Practical privacy-preserving outsourcing of biometric identification in the cloud," in European Symposium on Research in Computer Security, pp 186-205 2015
[14] X Du and H H Chen, "Security in wireless sensor networks," IEEE Wireless Communications Magazine, vol 15 no 4 pp 60-66 2008
[15] Y Zhu, T Takagi, and R Hu, "Security analysis of collusion-resistant nearest neighbor query scheme on encrypted cloud data," IEICE Transactions on Information and Systems, vol 97 no 2 pp 326-330 2014
[16] Mahender K, Kumar TA and Ramesh KS 2018 Analysis of multipath channel fading techniques in wireless communication systems *AIP Conference Proceedings* 1952() - 10.1063/1.5032012
[17] Rajasri I, Guptha AVSSKS and Rao YVD 2011 Influence of Structural Aspects on the Generation Process in Planetary Gear Trains *Engineering* 3(10) 1018-1021 DOI: 10.4236/eng.2011.310126
[18] C Zhang, L Zhu and C Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol 409 pp 56-67 2017
[19] Seena Naik K and Sudarshan E 2019 Smart healthcare monitoring system using raspberry Pi on IoT platform ARPN Journal of Engineering and Applied Sciences 14(4) 872-876
[20] Sudarshan, E, Satyanarayana, C and Bindu, CS, 2017, September A Parallel RLE Entropy Coding Technique for DICOM Images on GPGPU In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp 963-966) IEEE
[21] Sudarshan E, Naik K.S, Kumar P.P 2020 Parallel approach for backward coding of wavelet trees with CUDA. ARPN Journal of Engineering and Applied Sciences 15(9), pp.1094-1100
[22] Sallauddin M, Ramesh D, Harshavardhan A, Pasha SN and Shabana 2019 A comprehensive study on traditional AI and ANN architecture International Journal of Advanced Science and Technology 28(17) 479-487