2011 International Conference on Information and Network Technology
IPCSIT vol.4 (2011) © (2011) IACSIT Press, Singapore

Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security

Sowmya Suryadevara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anand Sharma

Mody Institute of Technology & Science, Lakshmangarh, Rajasthan, India

(sowmya.surya19, shuchita.kapoor, er.shweta89, rohailanaaz6)@gmail.com, (anand_glee)@yahoo.co.in

Abstract- Cloud computing is the need of changing network trends. It is based on the distributed computation in which the operations are carried out on the unfixed nodes. As all the nodes are not trusted so when the operations are applied on those nodes it hampers the users privacy information. So, in order to give it a secure environment we introduce tongue as a biometric to resolve the security issues of cloud computing. In this paper we are focusing on the method that has three parts:- user part provides tongue images; cloud initialization part has a tongue subspace and template database, cloud private matching identification part contains the core algorithm of the method which compares two encrypted numbers under double encrypted conditions. The algorithm ensures to make users tongue data secure and to develop a credible, efficient low complex method to guarantee cloud computing security.

Keywords-tongue recognition, secure cloud computing, matching identifier

1. Introduction

Cloud computing is the most promising and evolving network trend. However, a major characteristic of cloud computing is distributed computation based on unfixed nodes, operations often carried out without trusted nodes, so the calculation involved with user privacy information is insecure.

In this paper, we focus on how to solve the security issues of cloud computing. Cloud computing security based on private tongue recognition‘s significance is that tongue recognition will be applied to the cloud computing for the first time, supporting proof of private matching identification resolves security issues of cloud computing credibly, efficiently.

Calculation of tongue recognition and matching is under encrypted conditions, user sends a double encrypted tongue image to cloud, and cloud operates tongue recognition and matching under the encrypted conditions, the result is encrypted again before encrypted transmission to user [1]. In this way, cloud neither knows user’s real tongue data, nor which tongue and the tongue matches in templates, ensure no leakage of user privacy data.

Some people try to use the private biometric matching identification, especially in fingerprint and iris [8, 9, 10].However, these show more concerns on hardware architecture, such as biological data hash template is stored on the server. Server can know the result of matching (to only ensure the template is stored securely). In contrast, our scenario allows hide this information, and apply it to cloud computing .As far as we know, there is no helpful solution to solve the problem, when cloud computing involved with biometrics, efficiency and security problems appears.

2. Methodology

Assume that cloud is B, user is A. The diagram of our approaching method is summarized in Figure1.

Our method is divided into three parts: user, cloud initialization and private matching identification part of cloud. User part uses a series of tongue preprocessing method to do with original images, using Paillier [11] encryption algorithm encrypt processed images; cloud initialization part uses the processed original images to establish subspaces and tongue templates database through PCA [12] algorithm; cloud private matching identification part has projection, distance calculation, minimum distance finding [13] combined to achieve a tongue matching and recognition under encrypted conditions; cloud and user's communication is also in encrypted domain. Experimental results show that the method is credible and efficient to support cloud computing security study.

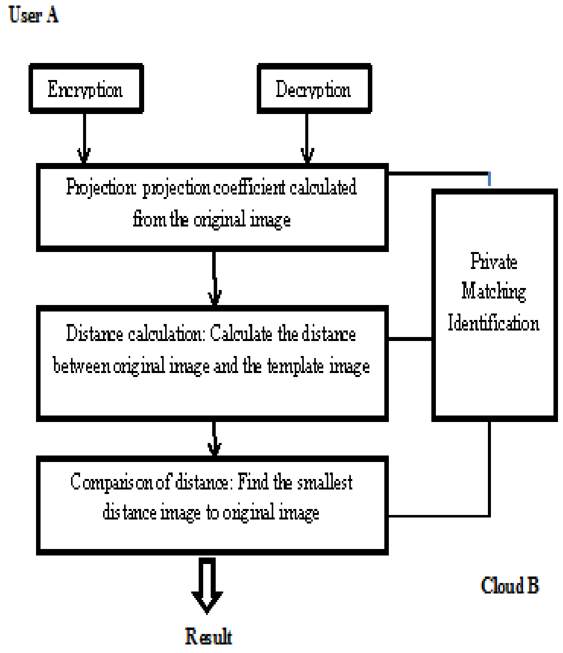

User A
Encryption
Decryption
Projection: projection coefficient calculated from the original image
Distance calculation: Calculate the distance between original image and the template image
Comparison of distance: Find the smallest distance image to original image
Private Matching Identification
Cloud B
Result

Figure 1: Method diagram.

A. User Part

A reads the original image, firstly preprocessing , then tongue detection and graying, also tongue vectoring, after double encrypting each pixel data, data is sent to B. Processing diagram is shown in Fig. 2 below:

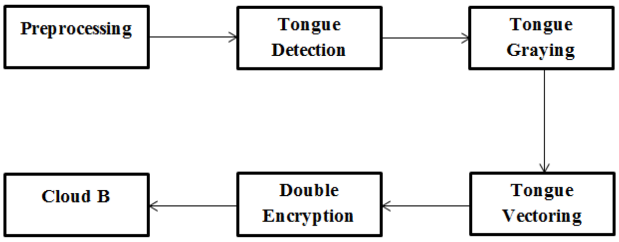


Figure 2: User processing diagram.

Preprocessing including image light, color, size, etc. makes the input of each original image uniform and consistent; tongue detection and graying contain finding the tongue region from original image, and cutting tongue down in unifying size, then convert each pixel's RGB three-color value to gray scale data; tongue vectoring transforms the two-dimensional tongue image to one-dimensional vector, Denoted as Γ , Double encryption firstly use Paillier encryption algorithm to encrypt each pixel's gray value, following paper presents "[]" on behalf of Paillier encryption process, Encryption will be denoted by vector .Then, use Elliptical encryption, Denoted by[[Γ]] , represent Elliptic encryption process in following paper with "[[ ]]".Finally, [[Γ]]is passed to B.

Encryption algorithm uses Paillier, because the Paillier encryption algorithm is additively homomorphic, and the encryption process is more simple and efficient. Paillier encryption algorithm is additively homomorphic because: [a] . [b] = [a + b], further: [ab] = [a]b. Cloud private matching identification are based on the above two properties.

Using Elliptic encryption for the distributed computation and poor security when communicating with cloud computing. Because the group protocol based on Elliptic encryption enables cloud and user’s communication data secure, credible, and complete when in an insecure, open network communication environment. Elliptic encryption is described as follows:

Step1. A selects an Elliptic curve Ep(a,b), y2= x3 + ax + b (mod p), and get a point on the Elliptic curve as point G.

Step2. A selects a private key k, and generates public key K=kG.

Step3. A sends Ep(a,b)and point K,G to B.

Step4.When B received the information, it will be encoded to be transmitted to the point M on Ep(a,b), and generates a random integer r(r<n).

Step5.B calculates points C1= M + rK; C2 = r.

Step6.B passes C1、C2 to A.

Step7.After receiving the information, A calculates C1-kC2; the result is the point M. Because C1-kC2 = M + rKk (rG) = M + rK - r(kG) = M, then the point M can be explicitly decode.

B. Cloud Initialization Part

The role of the part is to establish tongue subspace and the matching tongue templates database.

Suppose there are M tongue images for matching. After a series of preprocessing described above, like detection, graying, and vectoring to get M tongue vectors, denoted as Θ1,Θ2,….ΘM . Using PCA algorithm, the input data X is M individual tongue vectors, then obtain eigenvector matrixW, set W = [u1,u2,…..,uM], the matrix W’s , column k denoted as uk.

Use the formula y=WT(x-μ) to get projection coefficient of each face templates image Θi, denoted as Ωi and Ωi = [ωi1, ωi2,……, ωiM]T.

Pass the feature vector matrix W and the projection of each face templates’ coefficient Ωi to private matching identification part of cloud.

In order to ensure private matching identification simple, the mean face needs calculated, denoted by Ψ , is defined as Ψ=1/mΣi=1Θi . Finally, pass the mean face to private matching identification part.

C. Cloud Private Matching Identification Part

This part is the core of B, achieving face matching recognition in encrypted domain, using Paillier encryption algorithm and Elliptic encryption algorithm for double encryption.

This section is divided into three steps, namely, projection, distance calculation, minimum distance finding.

1) Projection

This step is to project the high-dimensional original data into lower-dimensional subspace, then obtain the projection coefficients of original face. Set data received by B is[Γ].

In the case of non-encrypted condition, firstly, using original one-dimensional face vector subtract the average face,namely:

$$\Phi = \Gamma' - \Psi = (\Gamma'_2 - \Psi_2)$$

|

|

$$(\Gamma'_x - \Psi_x) \qquad (1)$$

Then project to the subspace, namely:

$$\text{Л} = W^{T}\text{ф} \qquad (2)$$

Where л=[ω|1,ω|2,………,ω|m] and ω|Ґ= uҐT. ф = ф1.uҐ1+ ф2.uҐ2 +…..+фN.uҐN is the projection coefficient of input face and also a computing base for the following distance calculation.

But for B, to protect user privacy, the operation must be carried out in the encrypted domain. Because Paillier encryption algorithm is additively homomorphic, the following operations happen:

$$[\phi] = [\, Ґ{-}\Psi] = ([Ґ_2].[-\ \Psi_2\ ])$$

$$|$$

$$|$$

$$([Ґ_x].[-\ \Psi_x\ ]) \qquad (3)$$

So B's projection calculation becomes:

$$[\omega^{|}_{Ґ} = [\phi_1.u_{Ґ1+}\ \phi_2.u_{Ґ2} + \ldots..+\phi_N.u_{ҐN}] \qquad (4)$$
$$= [\phi_1]^{uҐ1.} \ldots.\cdot[\phi_N]^{uҐN},\ Ґ=1,2,\ldots\ldots,M$$

After the M times’ operation, B can receive encrypted projection coefficient [Ω].

As B knows Ψ and each u1, the operation is very convenient. More importantly, these operations are without A, face templates database will not be leaked to A. Operation of both sides doesn’t need the other’s participation, privacyinformation security will be guaranteed.

2) Distance Calculation

After receiving the input encrypted face projection coefficient [Ω], calculate the distance between the input face and each template in face templates database. Distance defined as:

$$D(\Omega,\ Л) = [\ \Omega\text{-}\ Л] \qquad (5)$$
$$= (\omega_2\text{-}\ \omega_1^{|})^2 + \ldots + (\omega_k - \omega_k^{|})$$
$$= \Sigma^{k}_{Ґ=1}\ \omega^{2}_{Ґ} + \Sigma^{k}_{Ґ=1}\ (-2\ \omega_Ґ\, \omega^{|}_{Ґ}) + \Sigma^{k}_{Ґ=1}\ \omega^{2|}_{Ґ}$$
$$= S_1+S_2+S_3$$

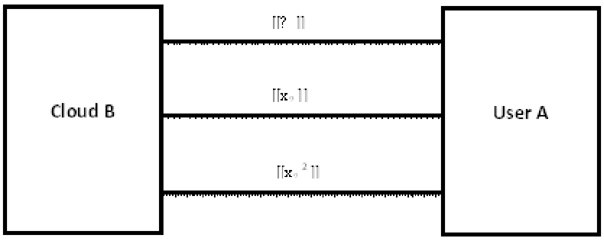
Distance formula is transformed into three-part, S1, S2, S3. Where S1= Σ In the encrypted domain, distance calculation becomes:

$$D[(\Omega,\acute{\Omega})]=[S_1].\ [S_2].\ [S_3]$$

It's easy to B to compute S1, because the projection coefficient ω1 of tongue templates is already known. B needs to calculate first S1, then encrypted by A’s public key.S2 calculation follows the formula:

$$[S_2] = \left[\sum_{i=1}^{K}(-2\omega_i\varpi_i)\right] = \prod_{i=1}^{K}[\varpi_i]^{-2\omega_i}$$

For S3, the computation is slightly complex, which requires B and A’s collaboration. First, B generates a random number η for each ω| , followed with Paillier encrypted, then calculates [xҐ]=[ωҐ+ ηҐ]=[ωҐ][ηҐ], transform into [[xҐ]]using Elliptic encryption. Random number η can increase ambiguity, so transmission doesn’t leak. Later, B sends M [[xҐ]] to A. [[xҐ]] decrypted by A with their own private key to xҐ obtain and xҐ2, double encrypted to [[xҐ]] , then pass to B. Following diagram Fig. 3 show the transmission:



When B obtains [[xҐ2]], decrypt to [xҐ2], then process obeys below:

$$[x_Ґ{}^2]\ .\ [\omega^{|}_{Ґ}]^{-2\eta}.\ [-\ \eta^2] = [(\omega^{|}_{Ґ+}\ \eta)^2\text{-}2\eta\omega^{|}_{Ґ\text{-}}\eta^2]$$
$$= [\omega^{|}_{Ґ}{}^{2}]$$

Later, multiply together each [ω|Ґ2] to compute [S2]. Note’s calculation performs only once. The computation of distance between each template and input tongue can directly use [S2].

Each tongue template performs the above algorithm to obtain each template’s distance with the input tongue [DҐ] = [[D=(Ω,Ώ)]. The implementation of the algorithm is in the encrypted domain.

3) Minimum Distance Finding

When the distances [DΓ] (Γ=1,2,….m) are calculated complete, begin to find the shortest distance among M encrypted distances. Tree structure is used to obtain the minimum distance , M distances are first divided by even and odd neighboring into M/2 groups, each group will leave the smaller one, reject the bigger one, then remain M/2 distances. Follow the above flow, the minimum distance can be found.

The key to the issue is to compare [DΓ] and in other words, to compare the two encrypted numbers and [b]. To solve the issue, the algorithm is as follows:

Step1.B produces a random number *r*, encrypted to[*r*];

Step2.B passes [a+r]=[a][r] and [b+r]=[b][r] to A;

Step3.A decrypt, obtain *a*+*r* and *b*+*r*, subtract the two numbers, if result is negative, then γ=1,, otherwise γ=0;

Step4. A passes [γ] to B;

Step5. B brings [γ] to the following formula:

$$[\gamma]^{[a]/[b]} . [b] = [(a< b) . (a - b) + b] = [m]$$

The result [m] is the smaller one of a and b‘ scipher text, show the credible, efficient result of comparing two encrypted numbers.

Finally, Elliptical encryption algorithm encrypts the smaller number based on the above method, obtain [[m]], then pass [[m]] back to A, A uses private key to decrypt [[m]], soon knows result.

3. Conclusion and Future Work

This paper focuses on the fast-developing cloud computing security issue, combined with tongue recognition, presents a creative method called cloud computing security based on private tongue recognition, which is a way to solve the issue. The core of the method is proposed to compare numbers in the encrypted domain, allow user obtain same, correct result as under non-encrypted conditions. The method proves to be credible, efficient, low-complex, and supports further study of cloud computing security.

We have used PCA algorithm for tongue recognition, and algorithm having higher recognition rate appears, due to the higher complexity of these algorithms, it’s difficult to apply to encrypted domain, so we leave this as our future work; and we will modify the implemented algorithms using multiple threads to improve performance of the algorithms.

4. References

[1] Blake, I.F., Kolesnikov, V.: Conditional Encrypted Mapping andComparing Encrypted Numbers. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 206–220. Springer, Heidelberg (2006)

[2] Yao, A.C.-C.: Protocols for Secure Computations (Extended Abstract).In: Annual Symposium on Foundations of Computer Science – FOCS 1982, November 3-5,pp. 160–164. IEEE Computer Society Press, Los Alamitos (1982)

[3] Goldreich, O., Micali, S., Wigderson, A.: How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In: ACM Symposium on Theory of Computing – STOC 1987, May 25-27, pp. 218–229. ACM Press, New York (1987)

[4] Jacobsson, M., Juels, A.: Mix and match: Secure function evaluation via ciphertexts.In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 162–177.Springer, Heidelberg (2000)

[5] Kruger, L., Jha, S., Goh, E.-J., Boneh, D.: Secure function evaluation with ordered binary decision diagrams. In: Proceedings of the 13th ACM conference on Computer and communications security CCS 2006, Virginia, U.S.A, pp. 410–420. ACM Press, New York (2006)

[6] Naor, M., Nissim, K.: Communication complexity and secure function evaluation. Electronic Colloquium on Computational Complexity (ECCC), 8(062) (2001)

[7] Naor, M., Nissim, K.: Communication preserving protocols for secure function evaluation. In: ACM Symposium on Theory of Computing, pp. 590–599 (2001)

[8] Kevenaar, T.: Protection of Biometric Information. In: Security with Noisy Data,pp. 169–193. Springer, Heidelberg (2007)

[9] Ratha, N., Connell, J., Bolle, R., Chikkerur, S.: Cancelable biometrics: A case study in fingerprints. In: Proceedings of the 18th International Conference on Pattern Recognition (ICPR), vol. IV, pp. 370–373. IEEE Press, Los Alamitos (2006)

[10] Tuyls, P., Akkermans, A.H.M., Kevenaar, T.A.M., Schrijen, G.-J., Bazen, A.M., Veldhuis, R.N.J.: Practical biometric authentication with template protection.In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546,pp. 436–446. Springer, Heidelberg (2005)

[11] Damg°ard, I., Jurik, M.: A Generalization, a Simplification and some Applications of Paillier's Probabilistic Public-Key System. Technical report, Department of Computer Science, University of Aarhus (2000)

[12] Turk, M.A., Pentland, A.P.: Face recognition using eigenfaces. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 586–591(1991)

[13] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," Privacy Preserving Technologies, LNCS, vol. 5672, pp. 235–253, 2009.

[14] The Database of Faces, (formerly'The ORL Database of Faces') AT&T Laboratories Cambridge,