Asian Journal of Computer Science and Technology
ISSN: 2249-0701 Vol.8 No.S3, 2019, pp. 128-132

Providing Security to Ensure Biometric Identification System in Cloud

Bhuvaneswari Kotte[1] and T. Sirisha Madhuri[2]
[1]PG Student, [2]Assistant Professor,
[1&2]Department of Computer Science and Engineering, School of Engineering and Technology,
Sri Padmavati Mahila Visva Vidyalayam, Tirupati, Andhra Pradesh, India
E-Mail: bhuna1205@gmail.com, talapurusirisha@gmail.com

***Abstract* - Biometric identification has rapidly growing in recent years. With the development of cloud computing, database owners are incentivized to outsource the bulk size of biometric data and identification tasks to the cloud to liberate the costly storage and computation costs, which however brings potential attacks to users' privacy. In this paper, we propose an adequate and security to keep biometric identification outsourcing scheme. Categorically, the biometric data is encrypted and outsourced to the cloud server. To get a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud implements identification operations over the encrypted database and returns the result to the database owner. An exhaustive security analysis indicated the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with antecedent protocols, experimental results show the proposed scheme achieves a better performance in both preparation and identification procedures.**

Keywords: **Biometric Identification, Cloud, Model and Design Goals, Security Analysis**

I. INTRODUCTION

Biometric identification has raised more and more attention; since it provides a promising thanks to establish users. Compared with ancient authentication strategies supported passwords and identification cards, identity verification is considered to be a lot of reliable and convenient[1]in addition, biometric identification has been wide applied in many fields by exploitation biometric traits like fingerprint [2],iris[3] and facial patterns[4]which may be collected from various sensors[5]-[9].

In a biometric authentication system, the information owner such as the Federal Bureau of Investigation United Nations agency is accountable to manage the national fingerprints information, could want to source the big biometric information to the cloud server (e.g., Amazon) to urge rid of the valuable storage and computation prices. However, to preserve the privacy of biometric information, the biometric information has to be encrypted before outsourcing. Whenever a FBI's partner (e.g., the police station) desires to attest associate individual's identity, he turns to the Federal Bureau of Investigation associated generates an identification question by victimisation the individual's biometric traits(e.g., fingerprints, irises, voice patterns, facial patterns etc.).Then, the Federal Bureau of Investigation encrypts the question and submits it to the cloud to find the shut match. Thus, the difficult downside is how to style a protocol that permits economical and privacy preserving biometric identification within the cloud computing.

Various protection saving biometric distinguishing proof arrangements [10]-[17] have been proposed. Be that as it may, the majority of them for the most part focus on protection conservation however overlook the productivity, for example, the plans dependent on homomorphic encryption and absent move for unique mark what's more, confront picture distinguishing proof separately. Experiencing execution issues of nearby gadgets, these plans are not productive once the measure of the database is bigger than 10 MB displayed a biometric ID conspire by using circuit plan and cipher text pressing methods to accomplish proficient ID for a larger information of up to 1GB [12]. In addition, Yuan and Yu [13] proposed an economical privacy-preserving biometric authentication scheme. Specifically, they created 3 modules and designed a concrete protocol to attain the protection of fingerprint rait to boost the potency, in their theme; the database owner outsources identification matching tasks to the cloud. However, Zhu *et al.,* [18] discovered that Yuan and Yu's protocol are often broken by a collusion attack launched by a malicious user and cloud. Wang *et al.*,[14] projected the theme Cloud BI-II that used random diagonal matrices to realize biometric authentication. However, their work was proven insecure in [15],[16].

In this paper, we have a tendency to propose an economical and privacy preserving biometric identification theme which may resist the collusion attack launched by the users and also the cloud. Specifically, our main contributions are often summarized as follows:

1. We inspect the biometric ID [13] conspire furthermore; demonstrate its inadequacies and security shortcoming under the proposed level-3 attack. In particular, we illustrate that the aggressor can recuperate their mystery keys by plotting with the cloud, and after that decode the biometric attributes everything being equal.
2. We present a novel proficient and security protecting biometric recognizable proof plan. The point by point security investigation demonstrates that the proposed plan can accomplish a required dimension of security assurance. In particular, our plot is secure under the

biometric distinguishing proof re-appropriating n show and can likewise oppose the assault proposed [18].

3. Compared with the current biometric distinguishing proof plans, the execution examination demonstrates that the proposed plot gives a lower computational expense in both readiness and ID methodology. The rest of this paper is composed as pursues: displays the models and plan objectives. In area III, we give an overview and the security investigation of the past convention proposed by Yuan and Yu.

II. MODELS AND DESIGN GOALS

This section introduces the system model, attack model design goals and therefore the notations utilized in the subsequent sections.

A. System Model

Varieties of entities are concerned within the system as well as the information owner, users and therefore the cloud. The information owner holds an oversized size of biometric knowledge (i.e., fingerprints, irises, voice, and facial patterns etc.), which is encrypted and transmitted to the cloud for storage. When a user needs to spot him/her, a question request is being sent to the information owner. When receiving the request, the database owner generates a cipher text for the biometric attribute and then transmits the cipher text to the cloud for identification. The cloud server figures out the most effective match for the encrypted question and returns the connected index to the information owner. Finally, the information owner computes the similarity n between the question knowledge and therefore the biometric knowledge related to the index, and returns the question result to the user.

In our theme, we tend to assume that the biometric knowledge has been processed specified its illustration is wont to execute biometric match. While not loss of generality, similar to [17], [18] we tend to target fingerprints and use Finger Codes [19] to represent the fingerprints. a lot of specifically, a Finger Code consists of n parts and every part may be a l-bit number(typically n = 640 and l = 8). Given 2 Finger Codes x = [x1, x2,..., xn] and y = [y1, y2,...., yn], if their Euclidean distance is below a threshold ϵ, they're typically considered as a decent match, which suggests the 2 fingerprints are thought-about from constant person.

B. Attack Model

Above all else, the cloud server is viewed as "legitimate yet inquisitive" as depicted [13]-[15], [17].The cloud entirely pursues the planned convention, yet endeavours to uncover protection from both the database proprietor and the client. We accept that an aggressor can watch every one of the information put away in the cloud including the scrambled biometric database, encoded inquiries and coordinating outcomes. Also, the aggressor can act as a client to develop self-assertive inquiries. Hence, we classify the assault demonstrate into three levels as pursues:

1. *Level 1:* Attackers can just watch the scrambled n information put away in the cloud. This pursues the notable cipher text-just assault display [20].
2. *Level 2:* Notwithstanding the encoded information put away in the cloud, aggressors can get a lot of biometric attributes in the database D yet don't have the foggiest idea about the comparing cipher texts in the database C, which is like the known-hopeful assault display [21].
3. *Level 3:* Besides every one of the capacities in level-2, aggressors in level-3 can be substantial clients. In this manner, aggressors can produce whatever number distinguishing proof questions as could reasonably be expected and get the relating cipher texts. This assault pursues the known-plaintext assault display [20].

A biometric ID plot is secure on the off chance that it can stand up to the level-α (α ∈ {1, 2, 3}) assault. Note that that if the proposed plan can oppose level-2 and level- 3 attacks, it does not imply that the assailant can both be the legitimate client and watch some plaintexts of the biometric database at the same time. This modern assault is excessively solid and no powerful techniques are intended to guard against this sort of attack [14]. In this paper, we centre on the plot assault between a vindictive client and the cloud server. The connection between the plaintexts of the biometric database and the cipher texts is not known to the attacker, which is like the attacks demonstrate [14].

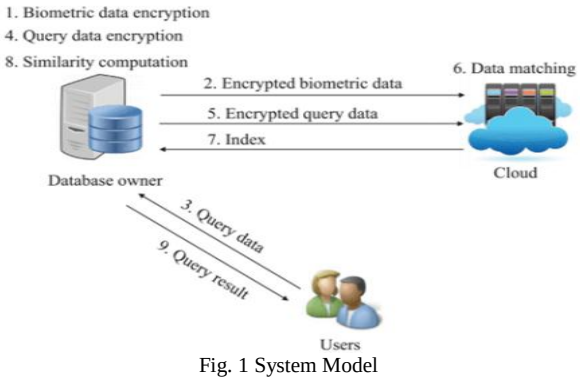

Fig. 1 System Model

C. Design Goals

So as to accomplish common sense, both security and effectiveness are considered in the proposed plan. To be increasingly explicit, structure objectives of the proposed plan are portrayed as pursues:

1. *Efficiency:* Computational expenses ought to be as low as conceivable at both the database proprietor side and the client side. To increase high productivity, most biometric distinguishing proof activities ought to be executed in the cloud.
2. *Security:* During the recognizable proof process, the protection of biometric information ought to be ensured. Attackers and the semi-honest cloud ought to get the hang of nothing about the delicate data.

D. Notations

Here, we list the main notations used in the remaining section as follows.

1. b_i − the i-th sample Finger Code, denoted as an n-dimensional vector bi = [bi1; bi2; .... bin].
2. B_i − the extended sample Finger Code of b_i, denoted as an (n + 1)-dimensional vector $B_i = [b_{i1}, b_{i2}, \cdot \cdot b_{i(n+1)}]$, where $b_{i(n+1)} = -0.5(b^2_{i1} + b^2_{i2} + \cdot \cdot \cdot + b^2_{in})$.
3. b_c − the query FingerCode, denoted as an n-dimensional vector $b_c = [b_{c1}, b_{c2},....,b_{cn}]$
4. B_c − the extended query FingerCode of b_c, denoted as an (n + 1)-dimensional vector $B_c = [b_{c1}, b_{c2},....,b_{c(n+1)}]$, where $b_{c(n+1)} = 1$.
5. W − the secret keys collection, denoted as W =(M1, M2, M3, H, R), where M1,M2 and M3 are (n +1) × (n + 1) invertible matrices, and H, R are (n + 1)-dimensional row vectors.
6. I_i − the searchable index associated with the i-th sample FingerCode b_i.

III. A NOVEL BIOMETRIC IDENTIFICATION SCHEME

In this area, we demonstrate the subtleties of the proposed biometric recognizable proof plan.

A. OverView

We develop a novel biometric distinguishing proof plan to address the shortcoming of Yuan and Yu's scheme [13]. To accomplish a more elevated amount of security assurance, another recovery way is developed to oppose the level-3 attack. In addition, we moreover remake the cipher text to decrease the measure of transferred information and enhance the productivity both in the arrangement and distinguishing proof techniques. In the rest of the piece of this segment, we will present the planning process and the ID procedure.

B. Preparation Process

In the planning procedure, $b_i$is the i-th test include vector gotten from the unique mark picture utilizing a component extraction calculation .To be progressively explicit, bi is a n-dimensional vector with l bits of every component where n = 640 and l = 8. For simplicity of distinguishing proof, b_i is stretched out by including a (n+ 1)- the component as B_i. At that point, the database proprietor scrambles B_i with the mystery key M_1 as pursues:

$$C_i = B_i \times M_1$$

The database proprietor further plays out the accompanying task:

$$C_h = M_2^{-1} \times H^T.$$

Each FingerCode B_i is related with a record I_i. After execute the encryption tasks, the database proprietor transfers (C_i , Ch, I_i) to the cloud.

C. Identification Process

The recognizable proof process incorporates the accompanying advances:

Step 1: When a client has an inquiry unique mark to be distinguished, he/she initially gets the question FingerCode b_c got from the inquiry unique mark picture. The FingerCode b_c is additionally a n-dimensional vector. At that point, the client sends b_c to the database owner.

Step 2: After accepting b_c, the database proprietor expands b_c to B_c by including a(n + 1) - th component equivalents to 1. At that point the database proprietor arbitrarily produces a (n + 1) × (n + 1) framework E. The i-th push vector Ei = $[E_{i1}, E_{i2}, \cdot E_{i(n+1)}]$ is set as an irregular vector, where the (n + 1)- th component is $(1 - \sum^{n}_{j=1} E_{ij} * H_j)/H_{n+1}$, $1 \le I \le (n + 1)$. From that point forward, the database proprietor plays out the accompanying calculation to cover up B_c:

$F_c = [E^T_1 * b_{c1}, E^T_2 * b_{c2}, \cdot E^T_{(n+1)} * b_{c(n+1)}]^T$

To safely send F_c to the cloud, the database proprietor needs to scramble F_c with the mystery keys and an irregular whole number r(r > 0). The calculation is executed as pursues: 0

$C_f = M^{-1}_1 \times r \times F_c \times M_2$.

At that point, the database proprietor sends C_f to the cloud for recognizable proof.

Step 3: After getting Cf from the database proprietor, the cloud starts to look through the FingerCode which has the base Euclidean separation with the question FingerCode Bc. P_i means the relative separation among B_i and B_c as pursues:

$P_i = C_i \times C_f \times C_h$

$= B_i \times M_1 \times M_1^{-1} \times r \times F_c \times M2 \times M_2^{-1} \times H^T$

$= B_i \times r \times F_c \times H^T$

$$= \sum_{j=1}^{n+1} r * bij * bcj$$

In above condition, the calculation result is a whole number, which can be utilized to look at two FingerCodes. For instance, to contrast the question b_c and two FingerCodes, state b_i and b_z, the cloud figures P_i and P_z, and plays out the accompanying task, where $1 \le i, z \le t$, $i \ne z$:

$P_i - P_z = \sum_{j=1}^{n+1} r * bij * bcj - \sum_{j=1}^{n+1} r * bzi * bcj$

$= (\sum_{j=1}^{n} r * bij * bcj - 0.5 \sum_{j=1}^{n} r * b_2 ij)$

$- (\sum_{j=1}^{n} r * bzj * bcj - 0.5 \sum_{j=1}^{n} r * b_2 zj)$

$= 0.5r(dist^2 zc - dist^2 ic)$.

As appeared in above condition, if $P_i - P_z > 0$, the cloud learns that b_i coordinates the question FingerCode much superior to b_z. Subsequent to rehashing the activities for the scrambled FingerCode database C in the cloud, the ciphertext C_i which has the least Euclidean separation with b_c can be found. The cloud further gets the comparing list I_i as indicated by the tuple (C_i, C_h, I_i) and sends it back to the database proprietor.

Step 4: After getting the list I_i , the database proprietor gets the relating test FingerCode b_i in the database D and computes the precise Euclidean separation between b_i furthermore, b_c as $dist_{ic} = \sqrt{\sum_{j=1}^{n}(bij - bcj)2}$. At that point, the database proprietor contrasts the Euclidean separation and the standard limit. On the off chance that the separation is not exactly the edge esteem, the inquiry is distinguished. Something else, the ID falls flat.

Step 5: Finally, the database proprietor restores the ID result to the client.

IV. SECURITY ANALYSIS

In this part, we initially demonstrate that our plan is secure under nlevel-2 and dimension 3 assaults, and afterward we will demonstrate the proposed plan can oppose the assault proposed by

A. Security Analysis under Level-2 Attack

As per the assault situation 2, an assailant can acquire some plaintexts of the biometric database, yet does not know the relating ciphertexts. We consider Ci which is acquired by increasing Bi and m1. Since the mapping connection among Bi and Ci is not known, it is inconceivable for the aggressor to figure Bi also, M1.

B. Security Analysis under Level-3 Attack

In the level-3 assault, other than the information of scrambled information in the cloud, the aggressor can fashion an expansive number of inquiry FingerCodes Γ as sources of info. In the accompanying, we will demonstrate the proposed plot is secure by demonstrating that the mystery keys can't be recouped. While intriguing with the cloud, the aggressor gets Cf and Ch, and after that plays out the accompanying task:

$$C_f \times C_h = M_1^{-1} \times r \times F_c \times M_2 \times M_2^{-1} \times H^T$$
$$= M_1^{-1} \times r \times F_c \times H^T$$
$$= M^{-1} \times r \times B^T.$$

Since r is a positive arbitrary whole number in recognizable proof process, the assailant can't register the mystery key M−1 1 straightforwardly. Imagining a substantial client, the assailant can build t inquiry FingerCodes $\Gamma = [b_1, b_2, \cdot \cdot b_t]$ reached out as $[B_1, B_2, \cdot B_t]$ for recognizable proof, which presents a lot of positive irregular values r_j and C_j , $1 \le j \le t$. Let P_j be the estimation of $C_j \times C_h$. The assailant registers P_j as pursues:

$P_j = M_1^{-1} \times r_j \times B_j^T$.

V. PERFORMANCE ANALYSIS

To evaluate the performance of the planned theme, we implement a cloud-based privacy-preserving fingerprint identification system. For the cloud, we tend to use a pair of nodes with 6-core 2.10 rate Intel Xeous processor and 32GB memory. We tend to utilize laptop with AN Intel Core a pair of 40 rate processor and 8G. Similar to the question Finger Codes area unit indiscriminately designate from the information that is made with random 640-entry vectors.

A. Complexity Analysis

Table a pair of summarizes the computation and communication costs on the information owner facet, cloud server and users in our scheme and also the themes [13] and [14] during this work, each matrix operation prices $O(n^3)$, wherever n denotes the dimension of a FingerCode, and also the sorting value of fuzzy Euclidean distances has time quality of O(m log m). As illustrated in Table a pair of, our theme has lower complexities in the preparation section. That is, a lot of computation and bandwidth prices will be saved for the information owner.

In the identification section, the computation quality of our scheme is below that in. The rationale is that our scheme performs vector-matrix multiplication operations to find the shut match, whereas must execute matrix- matrix multiplication operations. Though the quality of our theme is that the same as that in [we tend to emphasize that sacrifices the substantial security to realize such quick computation of Pi. Moreover, our theme executes fewer multiplication operations, and so obtains performance.

B. Experimental Evaluation

1. Preparation phase

It shows the computation and communication prices within the preparation part with the number of Finger Codes variable from one thousand to 5000. As shown, in our theme, registering 5000 Finger Codes needs 29.37s, which might save regarding eighty eight.85% and 90.58% time cost compared with severally. The reason is once encrypting a sample FingerCode, in our theme, only one matrix is required that results in fewer matrix multiplication operations. It shows the information measure prices of the 3 schemes. Since the information outsourced to the cloud is within the variety of vectors compared with matrices within the other 2 schemes, the communication price in our theme is much more.

2. Identification Phase

It shows the computation and communication prices within the identification part with the quantity of FingerCodes ranges from one thousand to 5000.As incontestable in fall schemes grow linearly because the size of information will increase. As in our theme fewer matrix multiplication operations area unit used it will save regarding 56% time price. The identification time can be saved the maximum amount as eighty four.75%, since the vector-matrix multiplication instead of the matrix-matrix multiplication operation is dead. The information measure prices of the 3 schemes, area unit nearly identical. The reason is that

everyone schemes have to be compelled to transmit a matrix within the identification part.

VII. RELATED WORKS

Related works on privacy-preserving biometric identification are provided during this section. Recently, some economical biometric identification schemes are projected. Wang and Hatzinakos projected a privacy-preserving face recognition theme [22]. Specifically, a face recognition methodology is designed by measure the similarity between sorted index numbers vectors. Wong and Kim[23] projected a privacy preserving biometric matching protocol for iris codes verification. In their protocol, it's computationally unfeasible for a malicious user to impersonate as Associate in nursing honest user. Barni *et al.*, [10] bestowed a FingerCode identification protocol supported the Homomorphic secret writing technique. However, all distances are computed between the questions and sample Finger codes within the info that introduces an excessive amount of burden as the size of fingerprints will increase. To boost the potency Evans *et al.*, [12] projected a unique protocol that reduces the identification time. They used Associate in nursing improved Homomorphic encryption rule to work out the geometrician distance and designed novel incoherent circuits to seek out the minimum distance.

By exploiting a backtracking protocol, the simplest match Finger Code will be found. However, [12] the entire encrypted database has got to be transmitted to the user from the info server. Wong *et al.*, [24] projected Associate in nursing identification theme based on kNN to realize secure search within the encrypted database. However, their theme assumes that there's no collusion between the consumer facet and cloud server facet. Yuan and Yu [13] proposed an efficient privacy-preserving biometric identification theme. However, Zhu et al., [18] pointed out their protocol will be broken if a malicious user colludes with the cloud server within the identification method. Based on, [13] Wang et al., conferred a privacy-preserving biometric identification theme in [14] that introduced random diagonal matrices, named Cloud BI-II. However, their theme has been verified insecure in [15],[16]. Recently, Zhang *et al.*, [17] proposed an efficient privacy-preserving biometric identification scheme using perturbed terms.

VIII. CONCLUSION

In this paper, we tend to planned a completely unique privacy-preserving biometric identification theme within the cloud computing. To realize the potency and secure necessities, we've designed a new coding rule and cloud authentication certification. The elaborate analysis shows it will resist the potential attacks. Besides, through performance evaluations, we additional incontestable the planned theme meets the efficiency want well.

REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, "Biometric identification," *Communications of the ACM*,Vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, "Fingerprint identification technology, "*Biometric Systems*, pp. 22-61, 2005.

[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] 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.

[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] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, Vol. 5, No.1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications Magazine*, Vol. 15, No. 4, pp. 60-66, 2008.

[8] 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.

[9] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," *In Proc. of IEEE GLOBECOM 2010*, pp. 1-5, 2010.

[10] M. Barni, T. Bianchi, and D. Catalano, *et al*., "Privacy-preserving fingercode authentication," *In Proceedings of the 12th ACM workshop on Multimedia and security*, pp. 231-240, 2010.

[11] M. Osadchy, B. Pinkas, and A. Jarrous, *et al*., "SCiFI-a system for secure face identification," *In Security and Privacy (SP), 2010 IEEE Symposium on*, pp.239-254, 2010.

[12] D. Evans, Y. Huang, and J. Katz, *et al*., "Efficient privacy-preserving biometric identification," *In Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011*.

[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] Q. Wang, S. Hu, and 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.

[15] Y. Zhu, Z. Wang and J. Wang, "Collusion-resisting secure nearest neighbour query over encrypted data in cloud," *In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on*, pp. 1-6, 2016.

[16] S. Pan, S. Yan, and W. Zhu, "Security analysis on privacy-preserving cloud aided biometric identification schemes," *In Australasian Conference on Information Security and Privacy*, pp. 446-453, 2016.

[17] 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.

[18] Y. Zhu, T. Takagi, and R. Hu, "Security analysis of collusion-resistant nearest neighbour query scheme on encrypted cloud data," *IEICE Transactions on Information and Systems*, Vol. 97, No. 2, pp. 326-330, 2014.

[19] A. Jain, S. Prabhakar, and L. Hong, *et al*., "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, Vol. 9, No. 5, pp. 846-859, 2000.

[20] H. Delfs, H. Knebl, and H. Knebl, "Introduction to cryptography," *Berlinetc: Springer, 2002*.

[21] K. Liu, C. Giannella, and H. Kargupta, "An attacker's view of distance preserving maps for privacy preserving data mining," *Knowledge Discovery in Databases*, pp. 297-308, 2006.

[22] Y. Wang, and D. Hatzinakos, "Face recognition with enhanced privacy protection," *In IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 885-888, 2009.

[23] K. Wong, and M. Kim, "A privacy-preserving biometric matching protocol for iris codes verification," *In Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC)*, pp. 120-125, 2012.

[24] W. Wong, D. Cheung, and B. Kao, *et al*., "Secure kNN computation on encrypted databases," *In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, pp. 139-152, 2009.