Security Attack on CloudBI: Practical privacy-preserving outsourcing of biometric identification in the cloud

Jiawei Yuan, Embry-Riddle Aeronautical University
Shucheng Yu, University of Arkansas at Little Rock

I. Introduction

In ESORICS 2015 [1], Wang et al. proposed a privacy-preserving outsourcing design for biometric identification using public cloud platforms, namely *CloudBI*. CloudBI introduces two designs: *CloudBI-I* and *CloudBI-II*. *CloudBI-I* is more efficient and *CloudBI-II* has stronger privacy protection. Based on the threat model of CloudBI, *CloudBI-II* is claimed to be secure even when the cloud service provider can act as a user to submit fingerprint information for identification. However, this security argument is not hold and *CloudBI-II* can be completely broken when the cloud service provider submit a small number of identification requests. In this technical report, we will review the design of *CloudBI-II* and introduce the security attack that can efficiently break it.

II. Brief review of *CloudBI-II*

In the data encryption phase of *CloudBI-II*, each FingerCode $b_i = [b_{i1}, b_{i2}, \cdots, b_{in}]$ are extended as B'_i

$$B'_i = \begin{bmatrix} b_{i1} & 0 & \cdots & 0 & 0 & 0 \\ 0 & b_{i2} & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_{in} & 0 & 0 \\ 0 & \cdots & 0 & 0 & -0.5\sum_{j=1}^{n} b_{ij}^2 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 \end{bmatrix}$$

Each B'_i is encrypted as

$$C_i = M_1 Q_i B'_i M_2$$

where M_1, M_2 are two random $(n+2)\times(n+2)$ invertible matrices, and Q_i is a random $(n+2)\times(n+2)$ lower triangular matrix with diagonal entries set as 1. All C_i will be outsourced to cloud servers.

$$Q_i = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ r_{21} & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_{(n+1)1} & \cdots & r_{(n+1)n} & 1 & 0 \\ r_{(n+2)1} & \cdots & r_{(n+2)n} & r_{(n+2)(n+1)} & 1 \end{bmatrix}$$

When the user submit a candidate FingerCode $b_c = [b_{c1}, b_{c2}, \cdots, b_{cn}]$ for identification, the biometric database owner extends it as B'_c

$$B'_c = \begin{bmatrix} b_{c1} & 0 & \cdots & 0 & 0 & 0 \\ 0 & b_{c2} & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & b_{cn} & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & 0 & r_c \end{bmatrix}$$

where r_c is a random number generated for each identification request. The owner then encrypts B'_c as

$$C_F = M_2^{-1} B'_c Q_c M_1^{-1}$$

where M_1^{-1} and M_2^{-1} are inverse matrices of M_1 and M_2 respectively, Q_c is a random $(n+2)\times(n+2)$ lower triangular matrix with diagonal entries set as 1. C_F is finally submitted to cloud servers for identification.

III. Security Attack on *CloudBI-II*

We now show that the cloud server only needs to submit more than 3 identification requests to break the ciphertext C_i of any FingerCode b_i in the owner's database. For expression simplicity, we use n' to denote $n+2$ in the rest part of this section.

After submitting an identification request, the cloud server has access to C_i of any FingerCode b_i and C_F of the submitted FingerCode b_c. Then, the cloud server can compute

$$P_i = C_i C_F = M_1 Q_i B'_i M_2 M_2^{-1} B'_c Q_c M_1^{-1} = M_1 Q_i B'_i B'_c Q_c M_1^{-1}$$

We now use P_1 of FingerCode b_1 as an example to show our attack, which can also be applied to any other FingerCode b_i in the same manner. In P_1, there are n'^2 unknowns in M_1, $n'-1$ unknowns in B'_1, $\frac{n'^2-n'}{2}$ unknowns in Q_1, $\frac{n'^2-n'}{2}$ unknowns in Q_c. As b_c is submitted by the cloud server, there is only one unknown r_c in B'_c. M_1^{-1} can be expressed with elements in M_1 since it is the inverse matrix of M_1. Among these unknowns, M_1, Q_1, B'_1 are fixed for all identification requests, B'_c and Q_c are randomly generated for each identification request. Therefore, after the first identification request, each new identification request only introduces $\frac{n'^2-n'}{2}+1$ unknowns to the computation of P_1. However, as $M_1, Q_i, B'_i, B'_c, Q_c, M_1^{-1}$ are all $n' \times n'$ matrices, it is easy to see that the cloud server can construct n'^2 equations for P_1 from each new identification request. As shown in Table III, when the cloud server submits more than 3 identification requests, it can construct more equations than the number of unknowns in P_1. Thus, all unknowns in P_1 decrypted by solving their corresponding equations. Once unknowns in B'_i are decrypted, the cloud can easily extract the actual FingerCode b_1. To decrypt any other FingerCode b_i, the cloud server just needs to perform the same attack as that for b_1.

To this end, we have demonstrated that *CloudBI-II* can be completely broken when the cloud server can submit more then 3 identification requests.

# of Requests	# of Unknowns in P_1	# of Equations from P_1
1	$2n'^2$	n'^2
2	$\frac{5n'^2}{2} - \frac{n'}{2} + 1$	$2n'^2$
3	$3n'^2 - n' + 2$	$3n'^2$
4	$\frac{7n'^2}{2} - \frac{3n'}{2} + 3$	$4n'^2$

TABLE I
Unknowns vs Equations

IV. Example of Security Attack on CloudBI-II

In this example, we set n=2 and n'=n+2=4. For $b_1 = [2, 2]$, the owner extends it as

$$B'_1 = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The owner randomly generates M_1, M_2, Q_1 as

$$M_1 = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} M_2 = \begin{bmatrix} 3 & 4 & 1 & 1 \\ 1 & 3 & 3 & 0 \\ 1 & 4 & 2 & 2 \\ 2 & 2 & 0 & 1 \end{bmatrix} Q_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{bmatrix}$$

B'_1 is encrypted as $C_1 = M_1 Q_i B'_1 M_2$ and outsourced to cloud servers. Now the cloud server selects $b_c = (1, 3)$ for identification and submits it 3 times. We denote the extended B'_c for 3 identification requests as B'_{c1}, B'_{c2}, B'_{c3} respectively.

$$B'_{c1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix} B'_{c2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} B'_{c3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 6 \end{bmatrix}$$

The owner encrypts B'_{c1}, B'_{c2} and B'_{c3} as $C_{F1} = M_2^{-1} B'_{c1} Q_{c1} M_1^{-1}$, $C_{F2} = M_2^{-1} B'_{c2} Q_{c2} M_1^{-1}$ and $C_{F3} = M_2^{-1} B'_{c3} Q_{c3} M_1^{-1}$ respectively, where Q_{c1}, Q_{c2} and Q_{c3} are randomly generated as

$$Q_{c1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 5 & 3 & 1 & 0 \\ 8 & 11 & 2 & 1 \end{bmatrix} Q_{c2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 5 & 12 & 1 & 0 \\ 2 & 8 & 3 & 1 \end{bmatrix} Q_{c3} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 12 & 1 & 0 & 0 \\ 10 & 0 & 1 & 0 \\ 3 & 2 & 1 & 1 \end{bmatrix}$$

After C_{F1}, C_{F2} and C_{F3} are sent to the cloud, the cloud compute

$$P_{11}M_1 = C_1 C_{F1} M_1 = M_1 Q_1 B_1' B_{c1}' Q_{c1} M_1^{-1} M_1 = M_1 Q_1 B_1' B_{c1}' Q_{c1} \tag{1}$$
$$P_{12}M_1 = C_1 C_{F2} M_1 = M_1 Q_1 B_1' B_{c2}' Q_{c2} M_1^{-1} M_1 = M_1 Q_1 B_1' B_{c2}' Q_{c2} \tag{2}$$
$$P_{13}M_1 = C_1 C_{F3} M_1 = M_1 Q_1 B_1' B_{c3}' Q_{c3} M_1^{-1} M_1 = M_1 Q_1 B_1' B_{c3}' Q_{c3} \tag{3}$$

Based on Eq. 1-3, the cloud can construct the following equations to solve all unknowns in M_1, Q_1, B_1', B_{c1}', B_{c2}', B_{c2}', Q_{c1}, Q_{c2} and Q_{c3}.

$$P_{11}M_1 = \begin{bmatrix} \frac{124}{3} & -24 & \frac{-68}{3} & \frac{68}{3} \\ 32 & -18 & -16 & 16 \\ 94 & -37 & -46 & 51 \\ \frac{190}{3} & -19 & \frac{-80}{3} & \frac{95}{3} \end{bmatrix} \times \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} = \begin{bmatrix} \frac{124}{3}x_1 - 24x_5 - \frac{68}{3}x_9 + \frac{68}{3}x_{13} & \cdots & \cdots & \frac{124}{3}x_4 - 24x_8 - \frac{68}{3}x_{12} + \frac{68}{3}x_{16} \\ 32x_1 - 18x_5 - 16x_9 + 16x_{13} & \cdots & \cdots & 32x_4 - 18x_8 - 16x_{12} + 16x_{16} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{190}{3}x_1 - 19x_5 - \frac{80}{3}x_9 + \frac{95}{3}x_{13} & \cdots & \cdots & \frac{190}{3}x_4 - 19x_8 - \frac{80}{3}x_{12} + \frac{95}{3}x_{16} \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{17} & 1 & 0 & 0 \\ x_{18} & x_{19} & 1 & 0 \\ x_{20} & x_{21} & x_{22} & 1 \end{bmatrix} \times \begin{bmatrix} x_{23} & 0 & 0 & 0 \\ 0 & x_{24} & 0 & 0 \\ 0 & 0 & x_{25} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & x_{26} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{27} & 1 & 0 & 0 \\ x_{28} & x_{29} & 1 & 0 \\ x_{30} & x_{31} & x_{32} & 1 \end{bmatrix}$$

$$P_{12}M_1 = \begin{bmatrix} \frac{4}{3} & -12 & \frac{-8}{3} & \frac{8}{3} \\ 0 & 6 & 0 & 0 \\ \frac{17}{3} & -21 & \frac{-7}{2} & \frac{16}{3} \\ 7 & 9 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} = \begin{bmatrix} \frac{4}{3}x_1 - 12x_5 - \frac{8}{3}x_9 + \frac{8}{3}x_{13} & \cdots & \cdots & \frac{4}{3}x_4 - 12x_8 - \frac{8}{3}x_{12} + \frac{8}{3}x_{16} \\ 6x_9 & \cdots & \cdots & 6x_{12} \\ \cdots & \cdots & \cdots & \cdots \\ 7x_1 + 9x_5 + x_9 + 2x_{13} & \cdots & \cdots & 7x_4 + 9x_8 + x_{12} + 2x_{16} \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{17} & 1 & 0 & 0 \\ x_{18} & x_{19} & 1 & 0 \\ x_{20} & x_{21} & x_{22} & 1 \end{bmatrix} \times \begin{bmatrix} x_{23} & 0 & 0 & 0 \\ 0 & x_{24} & 0 & 0 \\ 0 & 0 & x_{25} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & x_{33} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{34} & 1 & 0 & 0 \\ x_{35} & x_{36} & 1 & 0 \\ x_{37} & x_{38} & x_{39} & 1 \end{bmatrix}$$

$$P_{31}M_1 = \begin{bmatrix} \frac{980}{3} & -232 & \frac{-496}{3} & \frac{496}{3} \\ 192 & -138 & -96 & 96 \\ \frac{1792}{3} & -410 & \frac{-872}{3} & \frac{890}{3} \\ 218 & -156 & -106 & 112 \end{bmatrix} \times \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} = \begin{bmatrix} \frac{980}{3}x_1 - 232x_5 - \frac{496}{3}x_9 + \frac{496}{3}x_{13} & \cdots & \cdots & \frac{980}{3}x_4 - 232x_8 - \frac{496}{3}x_{12} + \frac{496}{3}x_{16} \\ 192x_1 - 138x_5 - 96x_9 + 96x_{13} & \cdots & \cdots & 192x_4 - 138x_8 - 96x_{12} + 96x_{16} \\ \cdots & \cdots & \cdots & \cdots \\ 218x_1 - 156x_5 - 106x_9 + 112x_{13} & \cdots & \cdots & 218x_4 - 156x_8 - 106x_{12} + 112x_{16} \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \\ x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{17} & 1 & 0 & 0 \\ x_{18} & x_{19} & 1 & 0 \\ x_{20} & x_{21} & x_{22} & 1 \end{bmatrix} \times \begin{bmatrix} x_{23} & 0 & 0 & 0 \\ 0 & x_{24} & 0 & 0 \\ 0 & 0 & x_{25} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & x_{40} \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ x_{41} & 1 & 0 & 0 \\ x_{42} & x_{43} & 1 & 0 \\ x_{44} & x_{45} & x_{46} & 1 \end{bmatrix}$$

Based on above matrix multiplications, it is clear that the cloud server can construct 16 equations for $P_{11}M_1$, 16 equations for $P_{12}M_1$, and 16 equations for $P_{12}M_1$. Meanwhile, there are 46 total unknowns in $P_{11}M_1$, $P_{21}M_1$ and $P_{31}M_1$. Thus, when the cloud server submit 3 identification requests, it will have sufficient information to solve all unknowns in M_1, Q_1, B_1', B_{c1}', B_{c2}', B_{c3}', Q_{c1}, Q_{c2} and Q_{c3}. Once the cloud server gets B_1', it can easily recover $b_1 = [2, 2]$.

REFERENCES

[1] Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, Minxin Du, and Zhibo Wang. Cloudbi: Practical privacy-preserving outsourcing of biometric identification in the cloud. In *ESORICS 2015*, volume 9327, pages 186–205. Springer International Publishing, 2015.