Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023

P2-BIS: PRIVACY-PRESERVING BIOMETRIC IDENTIFICATION SCHEME BASED ON A STATISTICAL INFERENCE ATTACK

G Devendra Babu[1], T Anil Kumar[2], K.Yatheendra[3]
[1]*P.G Scholor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: gdevendrababu7@gmail.com*
[2,3]*Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, ,*
[2]*Email:* anil.thumburu@gmail.com,[3]*Email:* k.yatheendra84@gmail.com

ABSTRACT

People can be identified by their distinctive physical characteristics using biometric identification. Fingerprinting is a well-known biometric identification method among these schemes. Many investigations connected with unique mark based biometric recognizable proof have been proposed; However, they are entirely based on robust cryptographic primitives like oblivious transfer and additively homomorphic encryption. Because of this, it is challenging to apply them to extensive databases. To determine this issue, a few plans have been suggested that depend on straightforward grid tasks instead of weighty cryptographic natives. As of late, Liu et al. proposed a superior grid based conspire utilizing the properties of symmetrical frameworks.
Regardless of being more proficient when contrasted with past frameworks, it actually neglects to give adequate protection from different sorts of aggressors. In this paper, we show that their plan is defenseless against an assailant who works with a cloud server by presenting factual derivation assault calculations. In addition, we present experimental results to show that our algorithms are both feasible and practical, as well as concrete identity confirmation parameters that an adversary must always pass.

Key Words: Homomorphic, Biometric, Dataset.

1.INTRODUCTION

Biometric identification is an easy way to identify users who belong to a particular group. To recognize clients, we use biometric characteristics as opposed to passwords, ID cards, and so forth. Because they are unique, always present, and highly invariant over time, it suffices to replace them. This implies that biometric characteristics fulfill three basic properties: permanence, singularity, and universality [1]. Because of this, biometric traits are frequently used in a variety of fields' identification and authentication systems. Simultaneously, be that as it may, the worries about protection proceed. In the event that a mystery key is produced from the biometric information is uncovered, it can't be reused or supplanted in a similar framework in view of its uniqueness. Notwithstanding this issue, there are many worries about security in biometric frameworks [2], [3], and various examinations have been led to determine this issue.[6].

A large portion of the distinguishing proof sytems referenced above require two fundamental calculations, an element extraction calculation [7]_[10], and a matching calculation [11]_[17]. The component extraction calculation is utilized to remove the elements of biometric qualities, for example, _fingerprints, palm veins, face, and irises. For instance, in the case of _finger prints, we first obtain the fingerprint image before employing the appropriate feature extraction algorithm to generate the n-dimensional vector known as Finger Code [18] from it. While maintaining privacy, the matching algorithm is used to compare Finger Codes. An examination of whether two Finger Codes are comparative is simple since it requires figuring the Euclidean distance between two vectors to check for similitude. Nonetheless, it isn't easy to compare them while saving protection. Since Finger Codes should be scrambled and an overall encryption conspire (like AES or RSA) requires a decoding cycle to register the Euclidean distance between them, we experience issues checking whether two encoded Finger Codes are indistinguishable.

Numerous works on privacy-preserving matching algorithms have been proposed as a solution to this issue. 12]_[15]. Barni et al. [12] proposed an additively homomorphic encryption fingerprint authentication method that preserves privacy. The index with the shortest distance between the candidate Finger Code and the Finger Code in the database is not the output of their scheme, but rather a set of indices that are within a certain threshold. By this cycle, the calculation cost is straightly expanded with respect to the size of the encoded information. Thus, their plan takes 16 s and utilizations 9.11 MB of transmission capacity for every ID solicitation to the data set (number of FingerCodeD320, length of the FingerCodeD16, and part size of the FingerCodeD7bits).

2.LITERATURE SURVEY

Early privacy-preserving biometric identification schemes only focus on the privacy-preserving issue. In these schemes, the biometric identification scheme is considered to be a two-party system, where the data owner takes charge of biometric dataset management and template matching. Most of these schemes are designed based on the secure computation protocol [18–20] and homomorphic encryption [9,21,22] techniques. Although the privacy-preserving is achieved in these schemes, the data owner is required to be equipped with powerful computing ability and remarkable storage capacity in these schemes, which can hardly be satisfied in most application scenarios and thus makes these schemes unpractical.

The emergence of cloud computing presents a new and promising paradigm to handle these challenges. Some researchers leverage cloud computing techniques to release the data owner from this burden. In their schemes, the data owner outsources the encrypted biometric dataset to the cloud server, and the matching process is completed on the cloud. Yuan et al. [6] proposed the first cloud-based privacy-preserving biometric identification scheme using a matrix encryption scheme, where the biometric dataset and identification query are both encrypted and sent to the cloud server by the data owner. However, Wang et al. [7] and Zhu et al. [23] pointed out that [6] is not secure under the known-plaintext attack model [24]. In addition, [7] presented a privacy-preserving biometric identification scheme based on the similarity matrix under the same system model in [6] and the security analysis showed that [7] had a higher security level than [6]. Zhang et al. [8] proposed an efficient privacy-preserving biometric identification scheme based on the matrix and perturbed terms with lower time cost and bandwidth consumption than [6,7]. Wang et al. [10] proposed an inference-based framework for privacy-preserving similarity search in Hamming space and achieved privacy-preserving biometric identification based on it. Hu et al. [25] proposed a privacy-preserving biometric identification scheme in an outsourcing environment with two noncolluded servers based on homomorphic encryption and batched protocols. With the help of the cloud, the computing cost of the data owner during the biometric matching is significantly reduced in the above schemes. However, in [6–8], the data owner has to keep on online to encrypt the user's query data and decrypt the identification result, which whittles some advantages of cloud computing away and leads heavy load to the data owner if it serves too many users at the same time. What is more, in all the cloud-based schemes above, the searching process is not optimized, which means that the searching cost of the cloud server is linear with the size of the dataset. Despite the fact that the cloud server is equipped with strong computing power, it may still run into a bottleneck while simultaneously severing too many users.

To address this issue, some researchers begin to focus on how to achieve sublinear searching efficiency in the biometric identification process, which will significantly ease the pressure of the cloud server. Zhu et al. [11] proposed a cloud-assisted privacy-preserving biometric identification scheme. With the help of an asymmetric scalar-product preserving encryption scheme and R-tree, sublinear search efficiency is achieved in [11]. Nevertheless, the data owner

also needs to keep online in [11]. And since R-tree is not constructed among the metric relation between the data objects, the cloud server needs to search the tree twice to find the closest biometric template in the dataset, which reduces the efficiency of the searching process. Yang et al. [26] proposed a privacy-preserving biometric identification scheme based on the M-tree to achieve a sublinear search efficiency.

3.SYSTEM ANALYSIS AND DESIGN

EXISTINGSYSTEM

Barniet al. [12] proposed a privacy preserving fingerprint authentication scheme using additively homomorphic encryption. The output of their scheme is the set of indices within some threshold, not the index having the minimum distance between the candidate FingerCode and the FingerCode in the database. By this process, the computation cost is linearly increased in proportion to the size of the encrypted data. As a result, their scheme takes 16 s and uses 9.11 MB of bandwidth for each identification request to the database (number of FingerCodeD320, length of the FingerCodeD16, and component size of the FingerCodeD7bits). SCiFI [13] is a secure component-based face identification system that matches images captured by the client to the images stored on the server. They built a secure-hamming distance and secure-minimum algorithm based on additively homomorphic encryption and 1-out-of-N oblivious transfer as cryptographic tools. These crypto- graphic tools enhance the security of the protocol, but reduce its efficiency.

In [13], the authors reported that the identification scheme takes 31 s of online computation for a database of 100 (a list of 100 faces representing a string of 900 bits). Consequently, this scheme is not suitable for practical biometric identification applications, because it is time-consuming to perform the identification algorithm for every request. In a similar work, Huang et al. [14] proposed a new protocol that improves the efficiency of the previous biometric identification schemes. They built an improved Euclidean distance protocol based on ciphertext packing techniques and use the encryption circuits to find the closest match. This scheme required 18 s with a 7.6 MB bandwidth cost per identification request on a 1 GB database. While it appears more efficient than the previous schemes, it has the problem wherein the client has to send the entire encrypted database to the server when identification is requested.Yuan and Yu [15] proposed a scheme that resolves the above problem. They use a simple matrix operation instead of heavy cryptographic tools to protect the owners' biometric information. This makes it possible to construct a practical
privacy-preserving biometric identification scheme. As a result, the authors report that it takes 4.31 s for an identification request over 10 GB. It is clear that the scheme is efficient but not secure. Zhu et al. [19] demonstrated that the scheme is not secure against collusion attacks between query clients and cloud servers. Moreover, they provide an upper bound of the

collusion-resistance ability of any accurate secure nearest neighbor (SNN) query scheme, which is a basic scheme used for most of the biometric identification schemes [20]_[22].

Disadvantages

- There is less security on outsourced data due to lack of strong Encryption scheme for to resist statistical inference attack.
- There is no Data Integrity Proof on outsourced data.

PROPOSED SYSTEM

In this paper, we show that their scheme is vulnerable to an attacker who colludes with the cloud server by introducing two statistical inference algorithms. Note that many previous works [12], [26], [27] related to biometric identification using homomorphic encryption schemes [28]_[30] have been proposed; however, for prac- tical reasons, we do not consider these schemes in this paper. Specifically, our contribution can be summarized as follows:

1) The system proposes statistical inference attack algorithms that can be applied to biometric identification schemes that use matrix operations with random numbers.

2) The system highlights the security flaw in Liu et al.'s scheme by applying our algorithm. By using this vulnerability, we show that the adversary can impersonate another user with a fake fingerprint.

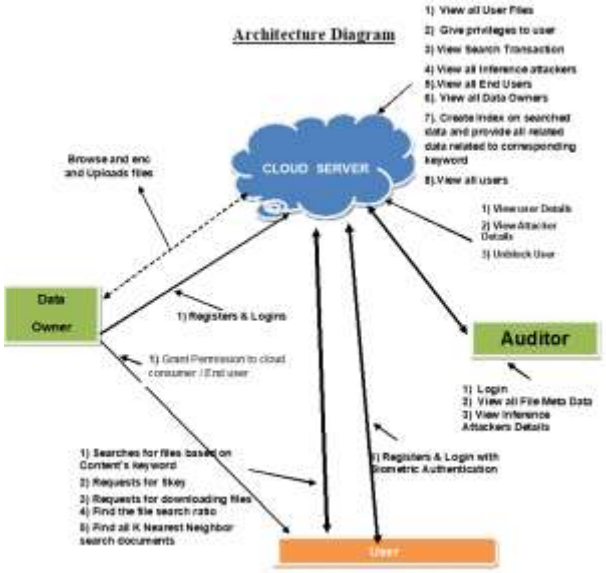
3) By providing concrete experimental results, we verify that our attack is practical. We also analyze each parameter in the attack algorithm, and then, propose optimized parameters efficiently to generate fake fingerprints.

Advantages

- The Data confidential is more due to Construction of Biometric identification for data access and identification for avoiding un authorized access.
- The system is more effective due to presence of Data Integrity Proof between the data owner and end user.

SYSTEM ARCHITECTURE

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 9, September : 2023



4. CONCLUSION

Privacy-preserving biometric identification schemes enable valid identification without any risk to private biometric information. Although these schemes have been researcher extensively, many concerns regarding security and efficiency remain. In this paper, we introduce new algorithms SIA and FFGA that generate fake fingerprint capable of passing the identification processes, and show that Liu et al.' scheme is not secure against a level-4 attacker who uses our pro- posed algorithms. Moreover, we provide an analysis of the attack complexity and experimental results to which concrete parameters were applied. In the future work, we plan to expand our attack and apply it to various biometric identification schemes, and we plan to design a privacy-preserving biometric identification that is secure against our attack.

REFERENCES

[1] R. Bolle and S. Pankanti, Personal Identi_cation in Networked Society: Personal Identi_cation in Networked Society, A. K. Jain, Ed. Norwell, MA, USA: Kluwer, 1998.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, ``Biometric recognition: Security and privacy concerns," IEEE Secur. Privacy, vol. 1, no. 2, pp. 33_42, Mar. 2003.

[3] N.K. Ratha, ``Privacy protection in high security biometrics applications,"inProc. ICEB (Lecture Notes in Computer Science), vol. 6005, A. Kumar and D. Zhang, Eds. New York, NY, USA: Springer, 2010, pp. 62_69.

[4] K. Nandakumar, A. K. Jain, and S. Pankanti, ``Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744_757, Dec. 2007.

[5] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, ``Privacy-preserving face recognition," in Proc. 9th Int. Symp.Privacy Enhancing Technol. Symp., 2009, pp. 235_253.

[6] A. Sadeghi, T. Schneider, and I. Wehrenberg, ``Ef_cient privacy-preserving face recognition," in Proc. Int. Conf. Inf. Secur.Cryptol., 2009, pp. 229_244.

[7] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, ``Filterbank- based _ngerprint matching," IEEE Trans. Image Process., vol. 9, no. 5, pp. 846_859, May 2000.

[8] S. Prabhakar and A. K. Jain, ``Decision-level fusion in _ngerprintveri_- cation," Pattern Recognit., vol. 35, no. 4, pp. 861_874, 2001.

[9] A. M. Bazen and S. H. Gerez, ``Systematic methods for the computation f the directional _elds and singular points of _ngerprints," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 905_919, Jul. 2002.

[10] H. Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans, and B. Gokberk, ``Fingerprint veri_cation using spectral minutiae representations," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 397_409, Sep. 2009.
[11] A. Ross, A. Jain, and J. Reisman, ``A hybrid _ngerprint matcher," Pattern Recognit., vol. 36, no. 7, pp. 1661_1673, Jul. 2003.
[12] M. Barni, F. Scotti, A. Piva, T. Bianchi, D. Catalano, M. Di Raimondo, R. DonidaLabati, P. Failla, D. Fiore, R. Lazzeretti, and V. Piuri, ``Privacy-preserving _ngercode authentication," in Proc. 12th ACM Workshop Multimedia Secur. (MM&Sec), New York, NY, USA, 2010, pp. 231_240.
[13] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, ``SCiFI_A system for secure face identi_cation," in Proc. IEEE Symp.Secur.Privacy, Oakland, CA, USA, May 2010, pp. 239_254.
[14] Y. Huang, L. Malka, D. Evans, and J. Katz, ``Ef_cient privacy-preserving biometric identi_cation," in Proc. NDSS, 2011, pp. 1_40.
[15] J. Yuan and S. Yu, ``Ef_cient privacy-preserving biometric identi_cation in cloud computing," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2652_2660.
[16] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, ``Privacy-preserving multi-keyword search ranked search over encrypted cloud data," in Proc. INFOCOM, May 2011, pp. 829_837.
[17] R. Li, Z. Xu,W. Kang, K. C. Yow, and C.-Z. Xu, ``Ef_cient multi-keyword ranked query over encrypted data in cloud computing," Future Gener.Comput. Syst., vol. 30, pp. 179_190, Jan. 2014.
[18] A. K. Jain, S. Prabhakar, and L. Hong, ``A multichannel approach to _ngerprintclassi_cation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 21, no. 4, pp. 348_359, Apr. 1999.
[19] Y. Zhu, T. Takagi, and R. Hu, ``Security analysis of collusion-resistant nearest neighbor query scheme on encrypted cloud data," IEICE Trans. Inf. Syst., vol. 97, no. 2, pp. 326_330, 2014.
[20] W. K. Wong, D. W.-L.Cheung, B. Kao, and N. Mamoulis, ``Secure kNN computation on encrypted databases," in Proc. 35th SIGMOD Int. Conf. Manage.Data (SIGMOD), 2009, pp. 139_252.