An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

ABSTRACT

Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users’ privacy. In this paper, we propose an efficient and privacy-preserving biometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourced to the cloud server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show the proposed scheme achieves a better performance in both preparation and identification procedures.

**EXISTING SYSTEM**

* Related works on privacy-preserving biometric identification are provided in this section. Recently, some efficient biometric identification schemes have been proposed. Wangand Hatzinakos proposed a privacy-preserving face recognition scheme [22]. Specifically, a face recognition method is designed by measuring the similarity between sorted index numbers vectors. Wong and Kim [23] proposed a privacy preserving biometric matching protocol for iris codes verification. In their protocol, it is computationally infeasible for a malicious user to impersonate as an honest user.
* Barni et al. [10] presented a Finger Code identification protocol based on the Homomorphic Encryption technique. However, all distances are computed between the query and sample Finger codes in the database, which introduces too much burden as the size of fingerprints increases.
* To improve the efficiency, Evans et al. [12] proposed a novel protocol which reduces the identification time. They used an improved Homomorphic encryption algorithm to compute the Euclidean distance and designed novel garbled circuits to find the minimum distance. By exploiting a backtracking protocol, the best match Finger- Code can be found. However, in [12], the whole encrypted database has to be transmitted to the user from the database server.
* Wong et al. [24] proposed an identification scheme based on kNN to achieve secure search in the encrypted database.
* **Disadvantages**
* The system doesn’t implement Biometric Identification Scheme.
* There is no an affective privacy preserving encryption techniques in this system.

**PROPOSED SYSTEM**

* The proposed system examines the biometric identification scheme [13] and shows its insufficiencies and security weakness under the proposed level-3 attack. Specifically, we demonstrate that the attacker can recover their secret keys by colluding with the cloud, and then decrypt the biometric traits of all users.
* The system presents a novel efficient and privacy-preserving biometric identification scheme. The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection. Specifically, our scheme is secure under the biometric identification outsourcing model and can also resist the attack proposed by the proposed system.
* Compared with the existing biometric identification schemes, the performance analysis shows that the proposed scheme provides a lower computational cost in both preparation and identification procedures.

**Advantages**

* An efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users.
* Attackers can only observe the encrypted data stored in the cloud. In order to avoid, the well-known cipher text-only attack model has been implemented.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java/J2EE(JSP,Servlet)
* Front End - J2EE
* Back End - MySQL