Biometrics-based cryptography scheme for E-Health systems

Hanlin Chen1*, Ding Ding1, Shuchun Su1, Jingyi Yin1

1 Department of Electronics and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing, 100070, China

*Corresponding author’s e-mail: hanlin_chen@sina.com

Abstract. Thanks to all-weather, effective and convenient services, E-Health Systems have been widely applied. However, with the increase of network risks and security threats, the privacy of personal medical information must be assured. The biometrics have become an effective and secure means of identification and authentication due to good distinctiveness and exclusiveness. To meet security and privacy requirements of E-Health systems, a biometrics-based cryptography scheme is proposed. First, Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) strictly identifies all components and operators in the whole system, and safely negotiate the cryptographic keys. Based on the biometrics of biological signals and the fuzzy vault algorithm, mutual authentications between the sensors and the terminal and between the terminal and the server can be achieved, and the keys for local and public communications are negotiated safely, ensuring the security of all communications. Second, Fingerprint-based Authority Access Mechanism (FAAM) is proposed to fulfil authority management, realizing secure storage and access of sensitive biomedical information in the system. Experimental results show that local communications within Wireless Body Area Networks (WBAN) and public communications have very high security, and personal medical information can be accessed safely.

1. Introduction

E-health applications of Wireless Body Area Networks (WBAN) have garnered great research interests in recent years. The occurrence of E-Health systems improves health data management as well as the whole healthcare systems due to high efficiency, high accuracy and broad availability [1,2]. This in-home healthcare system acquires biomedical information through sensors, and transmits them to remote healthcare provider to perform analysis and diagnosis, and take timely actions in case of necessity. Because biomedical information transmitted via networks encounters severe security and privacy threats, the privacy and confidentiality of personal information must be protected as mandated by the Health Insurance Portability and Accountability Act (HIPAA) [3].

The widely used biomedical information in E-Health applications has electrocardiogram (ECG), electroencephalogram (EEG), electromyogram (EMG) signals, face, iris, fingerprint, etc. A general architecture of E-Health systems is shown in figure 1. Wireless Body Area Networks (WBAN) are composed of bio-sensors, the terminal and local wireless networks. Patient’s biomedical signals are acquired by sensors and sent to the terminal via wireless network such as Bluetooth, Wi-Fi and ZigBee. The terminal could be a smart phone, handheld device, PC, Laptop, Tablet PC or custom-designed portable device. Through the terminal, these biomedical signals are transmitted to a remote server (often described as a Medical Server) for analysis and diagnosis via public networks such as mobile communication or internet, realizing the tele-monitoring of the patients [4].

However, there are various security problems at its every stage when an E-Health system works.
At the stage of local communication: Plain biomedical signals are transmitted from sensors to the terminal via wireless networks. Biomedical signals contain sensitive and private information about patients. Plain biomedical signals are prone to be eavesdropped, especially when transmitted via wireless network.

At the stage of terminal processing: The identity of the operators is not authenticated. Anyone can use the terminal to transmit own biomedical signals and view diagnostic results, which will seriously damage the privacy. Without any processing in the terminal, raw biomedical data is sent to the server even if they need an urgent protection.

At the stage of public communication: In public networks with more security risks, raw biomedical signals are transmitted directly. Personal information is easy to be eavesdropped, causing serious consequences, such as damage, disruption to operations or, in some scenarios, even loss of life.

At the stage of server processing: There is no authority management for data processing and storage. Both doctors and ordinary medical staff can access any information of patients, and storage security is not guaranteed.

Figure 1. A general architecture of E-Health systems

In this paper, we address the above issues by introducing the biometrics of biomedical signals. By ordinary cryptographic methods, we could only verify “what you possess” (e.g., an ID card) or “what you remember” (e.g., a password), but the biometrics overcome their deficiency and verify “who you are” instead. Because the biometrics have good distinctiveness and exclusiveness, that is, any two persons’ characteristics are sufficiently different, they could be used as a bio-signature [5]. Based on biological features, this paper proposes a biometrics-based cryptography scheme that could solve all security issues in the system. The scheme adopts Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) to strictly identify the sensors, the terminal and the server, and safely negotiate the communication keys, guaranteeing the legitimacy of the whole system and paving the way for cryptographic communications. Fingerprint-based Authority Access Mechanism (FAAM) is used for realizing secure storage and access of sensitive data. In this way, security risks at all stages of the system are eliminated, from local communications, terminal processing and public communications to final server processing.

The rest of the paper is organized as follows. Section 2 describes the proposed biometrics-based cryptography scheme. The implementation of the scheme is presented in Section 3. Section 4 shows results, and finally Section 5 concludes the paper.

2. The proposed biometrics-based cryptography scheme
To E-Health systems, security is top-drawer. To ensure high security, a biometrics-based cryptography scheme is proposed. The scheme is a comprehensive security scheme, which mainly includes Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) and Fingerprint-based Authority Access Mechanism (FAAM).
2.1 Biometrics-based Fuzzy Authentication and Key Negotiation

To high security, first of all, it is necessary to guarantee that all components and operators in the system are legitimate. In addition, the keys should also be negotiated during authentication to prepare for cryptographic communications. In the paper, Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) is proposed to fulfil identity authentication and key negotiation for E-Health systems.

2.1.1 Fuzzy vault secure sketch

In addition to good distinctiveness and exclusiveness, the biometrics also have “stable” variability, that is, any two samples from the same person may be different, but vary within a very small range over a period of time. Hence, a secure sketch called the fuzzy vault is needed for biometric-based authentication and key negotiation.

For precise reproduction of a noisy input ω, Juels and Sudan proposed a “fuzzy vault” secure sketch [6]. The secure sketch consists of a pair of algorithms (SS, Rec) that work as follows: on input ω, the algorithm SS outputs a help string S. Then, given S and the ω’ close to ω, the algorithm Rec can recover ω only if the set differences between ω and ω’ is less than or equal to an error tolerance t, realizing precise reproduction of the original input. Therefore, the sender of the string S could be authenticated by the receiver due to the distinctiveness and exclusiveness of the biometrics, and the key can be negotiated based on the restored original input. The help string S is secure in the sense that it does not reveal much about the original input ω: ω retains much of its entropy even if S is known. Thus, instead of storing ω for fear that later readings will be noisy, it is possible to store S instead, without damaging the privacy of ω.

2.1.2 Authentication and key negotiation for local communications

Before establishing cryptographic communications, all sensor nodes and the terminal in a WBAN must be authenticated, and key negotiation must be accomplished reliably. To order to realize the authentication and key negotiation of the WBAN, Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) using the biomedical signals is adopted. The sensors sample biomedical signals and extract the biometrics, then use the biometrics as the input ω of the algorithm SS of the fuzzy vault. The algorithm SS outputs a help string S and transfers it to the terminal. The terminal gets the biometrics ω’ of another sample from the patient’s biomedical signals stored beforehand in the terminal. Utilizing the help string S and the ω’, the algorithm Rec can precisely recover the original input ω only if the set ω and ω’ derive from the same patient, realizing mutual authentications between sensors and the terminal.

Besides, by using the same original biometrics ω, a secret key could be hidened and un-hidened. In this scheme, one sensor generates a random key and hides it with cryptographic fuzzy vault. The vault is then transferred to the terminal, which uses its own stored biometrics to un-hide the random key, thereby realizing the negotiation of communication keys between the sensors and the terminal.

2.1.3 Authentication and key negotiation for public communications

Similar to local communications, mutual authentications and key negotiation between the server and the terminal are also based on the biometrics of the patient’s biomedical signals. When the patient registers for monitoring services, a sample of her or his biomedical signals is acquired and stored in the server. After receiving the help string S from the terminal, the server extracts the biometrics ω’ of the patient’s sample signals. The algorithm Rec could recover the original biometrics from the terminal only if the set differences between the ω and the ω’ is less than or equal to an error tolerance t, that is, the ω and the ω’ come from the same person. Thus, mutual authentications and key negotiation between the server and the terminal could accomplished safely.

2.2 Fingerprint-based Authority Access Mechanism

Like biomedical signals, fingerprints are a very important and widely used biometric trait [7,8]. Based on fingerprint features, Fingerprint-based Authority Access Mechanism (FAAM) is proposed to address
secure storage and access of sensitive data. By the Fingerprint Matching [9,10], the operators could obtain different authorities, which corresponds to different access ranges. In the system, there are a large number of data files and multiple operators. Depending on different positions, different operators should access different range of files. In order to achieve secure access to files, different files define different access authorities, and different operators assign different access authorities. In this way, different operators can only access the files within their respective range, realizing security access of data files.

The files stored in the terminal can be accessed only if the operator pass the Fingerprint Matching, so the terminal is only used by the enrolled patient. In the monitoring center, doctors are authorized to access all data, including personal information of patients, diagnostic results, medical histories, ECG data, etc. Ordinary medical staff only have access authorities of diagnostic results and biomedical data. Nonmedical staff have no authority to access any data.

3. The implementation of the scheme

3.1 Overall implementation

According to the scheme, diagrammatic sketch of its implementation is shown as figure 2. The system contains three major blocks: sensors, terminal and monitoring center. There are two major communication links: local link from acquisition device to the terminal and public link from the terminal to the server. Under the effect of Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) and Fingerprint-based Authority Access Mechanism (FAAM), authorized access, local communication encryption, sensors and the terminal are firmly sealed in an independent WBAN, isolating from other WBANs absolutely. The security of public communications is guaranteed, and server system is tightly encapsulated also. Only the operators with different authorities can access the content corresponding to their authorities.

![Diagrammatic sketch of the proposed scheme](image)

Figure 2. Diagrammatic sketch of the proposed scheme

3.2 The implementation of the fuzzy vault algorithm

The implementation of the fuzzy vault algorithm is the core of the scheme. The fuzzy vault works by first acquiring the biological signals, extracting the biometrics and using the biometrics to generate a vault. This vault is then sent to the receiver, which tries to open it with its own biometrics. Only if the receiver's biometrics are common enough with the sender, i.e., the biometrics of the receiver and sender
come from the same person, the receiver will be able to open the vault and restore the original biometrics of the sender, realizing mutual authentication. Based on the restoring the biometrics, the vault could hide and un-hide a secret key, realizing key negotiation safely.

- **Algorithm SS:**
  1. The sender acquires the biomedical signals and applies some transformations to extract the biometrics $\omega$, $\omega = \{x_1, ..., x_p\}$.
  2. Generates a random key $K$.
  3. Divide the key $K$ into $p-t$ equal parts $a_0, a_1, ..., a_{p-t-1}$, and create a polynomial $F(z) = a_{p-t-1}z^{p-t-1} + a_{p-t-2}z^{p-t-2} + ... + a_0$, where $p-t-1$ is the order of a polynomial, and $t$ is an error tolerance.
  4. Compute the polynomial $F(z)$ at each biometrics point $x_j$ and obtain a set of ordered pairs $(x_j, F(x_j))$.
  5. Obfuscate this set of “legitimate” pairs by adding a large number of “chaff” pairs $(\text{ob}_k, \text{lg}_k)$ such that $\text{lg}_k \neq F(\text{ob}_k)$ to create a vault $S$.
  6. Transfers this vault $S$ to the receiver.

- **Algorithm Rec:**
  1. Apply the same transformations as the sender to obtain the biometrics $\omega'$ of biomedical signals, $\omega' = \{x_1', ..., x_p'\}$.
  2. Computes the intersection of the sets $\omega'$ and the first variables of each pairs in the received vault $S$, i.e. $\omega' \cap \{\omega \cup \{\text{ob}_1, \text{ob}_2, ..., \text{ob}_M\}\}$, where $M$ is the number of chaff points.
  3. If $|\omega' \cap \omega| \geq p-t$, then the receiver has enough number of $(x_j, F(x_j))$ pairs to reconstruct the polynomial $F(z)$ by using Lagrangian interpolation [11], deriving the polynomial coefficients $a_0, a_1, ..., a_{p-t-1}$.
  4. The terminal then concatenates the coefficients of the regenerated polynomial to obtain the key $K$.

4. Results

4.1 Results of Biometrics-based Fuzzy Authentication and Key Negotiation

Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) is used to ensure the legitimacy of all components and operators in the system, and negotiate communication keys safely. The sender acquires biological signals and derives the biometrics. Using the fuzzy vault, the biometrics hide a secret key $K$. As long as the receiver has the biometrics enough close to the sender, the receiver could open the vault and obtain the key $K$, realizing the authentication and key negotiation.

False acceptance rate (FAR) and false rejection rate (FRR) are used to evaluate the accuracy of the fuzzy vault. FAR is defined as the false acceptance percentage of illegitimate users, while FRR is the false rejection percentage of legitimate users. In the scheme, the error tolerance is $t$. Figure 3 shows the experimental results on FAR and FRR. When the error tolerance is 5, FAR is only 0.4% and FRR can reach 6.5%, which means that legitimate users can have a success rate of 93.5% on the basis that 99.6% of impostor users are identified. Hence, the fuzzy vault is very high security.
4.2 Results of Fingerprint-based Authority Access Mechanism

By utilizing Fingerprint-based Authority Access Mechanism (FAAM), only authorized medical staff can use the system to access patient's data and complete diagnosis. In the system, a great quantity of sensitive information will be involved, such as biomedical files, individual information of patients, diagnostic results, medical histories, the samples of the enrolled patients, etc. Medical staff at different ranks or even different Medical staff at the same rank should have different ranges of data access. By verifying fingerprints, medical staff can obtain different authorities to access different data. Authority access results are as shown in Table 1.

Table 1. Authority access management of the system

|                  | Biomedical files (Authority>4) | Diagnostic results (Authority>6) | The samples of patients (Authority>4) | Medical histories (Authority>6) | G1 Personal information (Authority=8) |
|------------------|--------------------------------|---------------------------------|-------------------------------------|-------------------------------|--------------------------------------|
| Doctor 1 (Authority=8) | ✓                              | ✓                               | ✓                                   | ✓                             | ✓                                    |
| Assistant (Authority=5) | ✓                              | ✓                               | X                                   | X                             | X                                    |
| Nonmedical (Authority=0) | X                              | X                               | X                                   | X                             | X                                    |

5. Conclusion

A biometrics-based cryptography scheme for E-Health systems is designed and implemented. Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) can guarantee the legitimacy of all components and operators in the system, and negotiate the communication keys, ensuring the security of network communications. Fingerprint-based Authority Access Mechanism (FAAM) realizes effective authority management. Only the operators with authorities can access the devices and data corresponding to their authorities. The experimental results show the scheme has good security and high performance, thus providing a secure, reliable, effective support for E-Health systems.
References

[1] Alvarez, R.C. (2002) The promise of e-health–a canadian perspective. Ehealth international, 1(1): 4-9.

[2] Jain, A.K., Ross, A., Prabhakar, S. (2004) An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1): 4-20.

[3] The Health Insurance Portability and Accountability Act (P.L.104-191). (1996) Enacted by the U.S. Congress.

[4] Zhai, X.J., Ali, A.A.S., Amira, A., Bensaali, F. (2017) ECG encryption and identification based security solution on the Zynq SoC for connected health systems. Journal of Parallel & Distributed Computing, 106: 143-152.

[5] Jain, A., Bolle, R., Pankanti, S. (2006) Biometrics: personal identification in networked society. Springer Science & Business Media, 479: 356-362.

[6] Juels, A., Sudan, M. (2002) A fuzzy vault scheme. In: IEEE International Symposium on Information Theory. Lausanne. pp. 408-415.

[7] Nandakumar, K., Jain, A.K., Pankanti, S. (2007) Fingerprint-based fuzzy vault: implementation and performance. IEEE Transactions on Information Forensics and Security, 2(4): 744-757.

[8] Yang, S., Verbauwhede, I. (2005) Automatic secure fingerprint verification system based on Fuzzy Vault scheme. In: Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’05). Philadelphia. pp. 18-23.

[9] Hrechak, A.K., McHugh, J.A. (1990) Automated fingerprint recognition using structural matching. Pattern Recognition, 23(8): 893-904.

[10] Jain, A., Lin, H., Bolle, R. (1997) On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4): 302-314.

[11] Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S. (2010) PSKA: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine, 14(1): 60 -68.