American Journal of Engineering Research (AJER)
E-ISSN: 2320-0847 p-ISSN: 2320-0936
Volume-8, Issue-2, pp-90-94
www.ajer.org
Research Paper Open Access

Wearable Medical Device Data Transmission System Based On Elliptic Curve Cryptography

Liufen Li[1],Zouyu Xie[1*], Zhengxi Wei[2]
[1]*School of mathematics and statistics, Sichuan University of Science and Engineering, Sichuan,China*
[2]*School of computer science, Sichuan University of Science and Engineering, Sichuan,China*
Corresponding Author: Zouyu Xie

ABSTRACT: With the rapid development and widespread popularity of smart wearable devices, the emergence of wearable medical devices has also brought great convenience to doctors and patients. However, the physical health status is private data, in order to prevent the data from being intercepted or tampered with during the process of transmitting data to the server, this paper proposes a data transmission scheme for the wearable medical device based on the ECC (Elliptic curve encryption) algorithm. The ciphertext transmission is implemented by an ECC algorithm, and the digital signature is generated from the ECC to verify the integrity of the data

KEYWORDS Wearable medical device,ECC, Ciphertext transmission,Digital signature

---

Date of Submission: 26-01-2019 Date of acceptance: 09-02-2019

I. INTRODUCTION

With the rapid development of information and communication technologies, the form and function of devices for information and communication products are also evolving. Since 2013, wearable devices have been around us. In 2014, it is called “the first year of wearable devices” [1-4], and the domestic and international markets quickly stimulated a new wave of wearable devices. In the subdivision of wearable devices, wearable medical devices have become another fast-growing market in the wearable technology branch, and its sustainability will further lead to a larger mobile medical market. Research institutes such as the School of Engineering and the Institute of Science and Technology at universities in Russia, France, the United Kingdom, Japan and Korea have specialized laboratories or research groups that focus on the research of wearable medical devices. Wearable medical health research in the late 1990s is almost in sync with international wearable medical device research. According to Frost & Sullivan's prediction, by 2020, chronic disease management and other clinical applications in the clinical-grade medical wearable device market will reach $18.9 billion, a compound annual growth rate of 29.9%. It can be seen that wearable medical equipment will become a revolutionary breakthrough in solving human health.

A wearable medical device is a portable medical or health electronic device that can be facing worn on the body to sense, record, analyze, regulate, intervene or even treat a disease or maintain a healthy state with software support. Lies in implanting the human body, binding the human body, and recognizing the physical characteristics and state of the human body. Always monitor our physical condition, exercise status, metabolic status, and let us dynamic, static life, physical characteristics of the data, Its real value is to let the physical condition digitization, wearable medical equipment can monitor blood sugar in real time, blood pressure, heart rate, blood oxygen, body temperature, respiratory rate and other human health indicators and basic treatment of the human. There are four main types of wearable medical devices, from simple to complex, passive monitors, monitoring devices, diagnostic devices and treatment devices [5-8].

But everything has two sides, and the more powerful and flexible things, the greater the security risks. The wearable medical device allows the doctor to more accurately and more accurately grasp the patient's information and the body's various privacy data, and also transmits the body's various privacy data to the server. When data is transmitted to the server through the network, the plaintext transmission or the use of encrypted transmission methods that are easily cracked, there is danger that the data is intercepted by the air, tampering, etc.. If the attacker has mastered or even falsified these private data, it will not only mislead doctors to make wrong judgments about patients'physical condition, thus causing misdiagnosis to threaten patients' lives, but also cause irreversible impact on patients'lives because of data leakage. For example: the physiological data source leaked. The attacker can analyze the health index of the user by analyzing the health data of the target user's heart rate and blood sugar. If the user's leaked health condition is something that is difficult to talk about (such as AIDS, hepatitis B, etc.), then he may be discriminated against or unfairly treated. Therefore, in order to ensure the security of data transmission, we need to study the security issues of wearable medical devices in the process of data transmission.

II. RELATED WORK

The development of Internet technology has brought people closer and closer together. It allows people to communicate various information regardless of where they are. The same is true for wearable medical devices. If you simply collect data and do not transfer the data to a doctor for processing and analysis, the device has no practical use. Therefore, how to safely and reliably transmit the collected data to the server, the doctor then observes the patient's physical condition through the server and gives corresponding advice to the patient, which is the most problem to be solved at present.

In terms of encryption algorithms, common encryption algorithms are mainly divided into three categories:

- Elliptic Curve Cryptography (ECC), an asymmetric cryptographic algorithm based on elliptic curve mathematics, which is based on discrete pairs based on elliptic curves. The number system on the cryptosystem[9-13].
- The information summary algorithm, under normal circumstances, different files will have different "digital fingerprints", and then will achieve the effect of digital signature. If the document changes, the original information summary will change. In 2012, Zhou Qinqin and others proposed a hardware implementation circuit for the more common information digest algorithm MD5 and SHA-1 encryption algorithm.
- The digital signature technology, the technology is mainly the organic fusion of the information digest algorithm and the asymmetric encryption algorithm, which can play an important role in verifying data integrity. In 2018, Song Jingwen et al. designed a signature scheme that can satisfy the characteristics of verifiability, distinguishability and unforgeability by analyzing the existing SM2-based proxy signature scheme.

In practical applications, Quynh Dang introduced FIPS 180-3 and FIPS 180-4 federal information processing standards in 2013 in the "Changes in Federal Information Processing Standard (FIPS) 180-4, Secure Hash Standard" article. Two new secure cryptographic hashing algorithms are specified in FIPS 180-4: Secure Hash Algorithms SHA-512/224 and SHA-512/256 in 2018, Zhao Ruifen et al. in Cloud Computing System-Based Data An improved hybrid encryption algorithm is proposed in the article "Transportation Security for Storage Security" , and the processing strategy after data transmission interruption is added to ensure security during data transmission. In the same year, Song Xiaorui and others studied the existence of various security vulnerabilities such as WEP, WPA-PSK (TKIP) and WPA2-PSK (AES), and proposed a high-security hybrid encryption security based on WIFI. algorithm. The algorithm combines algorithms such as RSA, AES and SHA-256 to encapsulate the transmission information .

However, the IoT technology based on wearable devices requires the integration of cryptography technology to ensure the security of the transmission of private data between the server and the wearable medical device.

III. PRELIMILARIES

1. In $GF（p）$ Elliptic curve on：Let $GF（p）$ be a finite field where the characteristic p is a large prime number， $a，b \in GF（p）$ and satisfy $4a3+ 27b2 \neq 0$。Therefore the elliptic curve satisfies the equation $2=x3+ax+b$ ，All points on the elliptic curve (including infinity points) constitute an additive group. Given an elliptic curve， We define $P=（x1，y1）$， $Q=（x2，y2）$， Since the elliptic curve is symmetric about the x-axis, $-P=（x1,-y1）$， Define $R=P+Q$ as the point where the elliptic curve P and Q intersect the elliptic curv.Hypothesis $R=（x3，y3）$ ， then $x3=\lambda 2-x1-x2$， $y3=\lambda（x1-x3）-y1$， whwere,

$$\lambda=\frac{y_2-y_1}{x_2-x_1}$$

2. Discrete logarithm problem for finite fields (ECDLP)：Given the prime number p and the elliptic curve E, taking an elliptic curve point P, and a random number k such that a point $Q = kP$, that is, a known P point and a random number k, it is easy to find the Q point. However, known that Q and P are difficult to find k.
3. Key Generation of Elliptic Curve on $GF（p）$: Select a Generator $G =（x1，y1）$ on the curve whose order is n and n is a large prime number. The data owner randomly selects an integer d in $[1，n-1]$ and calculates $Q = dG$. At the same time, he publishes his public key $（G，Q，Ep（a，b），n）$ and holds his private key $（d）$.
4. Elliptic curve encryption of $GF（p）$: The data owner calculates the point of the data visitor by looking up the public key $（G，Q，Ep（a，b），n）$ of the data visitor and representing the message m as a domain element $m \in Fq$, and randomly selecting an integer k on the interval $[1，n]$, and calculating the point by the public key of the data visitor $（x1，y1）= kG$, then calculate the point $（x2，y2）= kQ$, here cannot let $x2 = 0$. Otherwise, re-randomly select the integer k, calculate $C = m * x2$ here, and then generates$（（x1，y1），C）$.
5. Decryption of elliptic curve on $GF（p）$: The data requester decrypts the obtained ciphertext data $（（x1，y1），C）$ by its own private key d, and calculates $（x2，y2）= d *（x1，y1）$ by calculating $m = C * x2 - 1$.
6. Elliptic curve digital signature on $GF（p）$: The data owner randomly selects an elliptic curve $Ep（a'，b'）$, and publishes his own public key $（GF（p），G'，Q'，n'）$, owns the private key $（d'）$, and now the data owner performs the following steps

1） randomly select an integer $k \in Z*n'$;

2） calculate $kG' =（x1'，y1'）$, $r = x1 \bmod n'$, if $r = 0$ then re-select k;

3）calculate the one-way hash SHA-1 function: $e = SHA - 1（m）$;

4）calculate $s = k - 1（e + dr）\bmod n'$, if $s = 0$, then reselect k;

7. Signature verification:

1） verify that r, s is an integer in $[1，n' - 1]$;

2）calculation $e = SHA\text{-}1（m）$;

3）calculation $w = s - 1 \bmod n'$;

4）calculation $u1 = e * w（\bmod n'）$, $u2 = r * w（\bmod n'）$;

5） calculation $X = u1G + u2Q =（x1，y1）$, if $X = 0$, then reject the signature, calculate $r' = x1（\bmod n'）$, if $r' = r$, then accept the signature, otherwise reject.

IV. WEARABLE MEDICAL DEVICE DATA ENCRYPTION TRANSMISSION SYSTEM

Preparation Phase. The doctor enters $\left(Q, G, GF(p), n\right)$ four public key parameters, announces the public key P_1, and holds the private key d_1. After the patient gets the medical device, enter $\left(Q', G', GF(p), n'\right)$ four public key parameters, tell the doctor the public key P_2, and holds the private key d_2.

Step1: When the data (m) transmitted by the user starts transmission through the device, the device encrypts the data through the public key of the doctor confirmed by the user to generate ciphertext $P_1\text{-}m$.

Step2: The patient's device generates a digital signature $（r，s）$.

Step3: Digital signature $（r，s）$ and ciphertext $P_1\text{-}m$ arrive at the server through a specified transport channel.

Step4: The doctor first downloads the digital signature $（r，s）$ from the server and checks whether r and s in the digital signature are integers in $[1，n' - 1]$. If not, feedback the server. Yes, go to the next step,

Step5: The doctor downloads the ciphertext P_1-m and decrypts it by the private key to obtain the plaintext m'.

Step6: The doctor calculates X by plaintext m', and if $X = 0$ returns the server, if not, proceed to the next step.

Step7: The doctor calculates whether the r' is correct by using the plaintext m'. If it is not correct, the server is fed back. If it is correct, confirm m'=m. The doctor gives treatment advice to the patient through the data.

Wearable medical device encrypted data transmission system is shown in Fig.1.

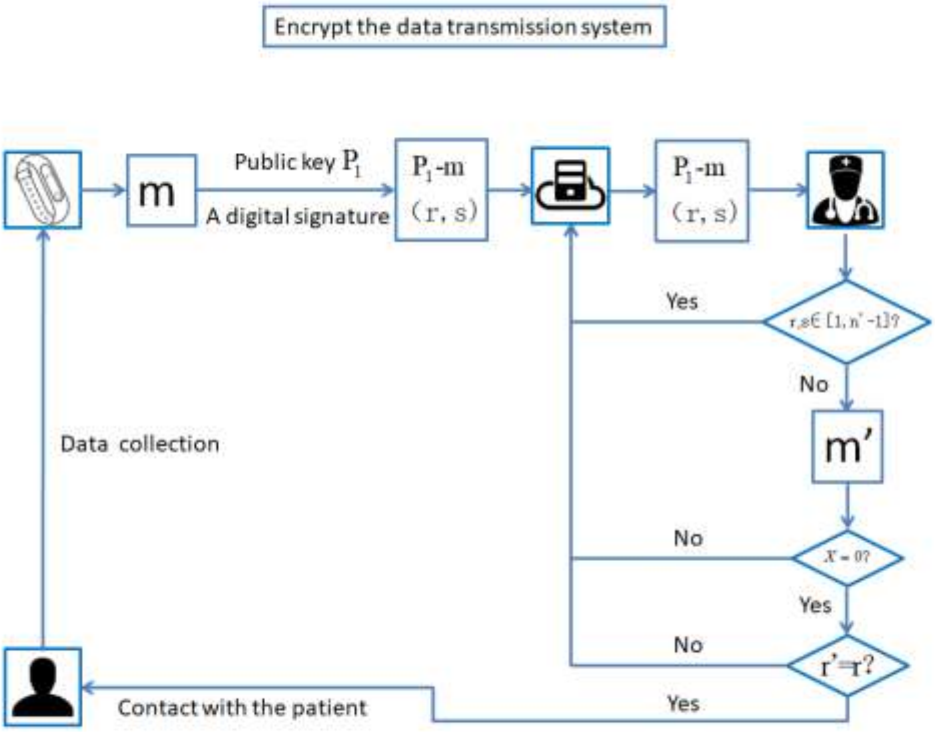

Fig.1. Encrypt the data transmission system

V. CONCLUSION

In this paper, the ellipse encryption algorithm is applied to the data transmission system of the wearable medical device. The encryption algorithm can effectively and quickly ensure the security of the data in the transmission process, and to a certain extent, ensure that the transmission data will not be monitored and falsified. It makes the wearable medical device safer and more convenient for the patient, so that the doctor can understand the patient's physical condition more timely.

ACKNOWLEDGEMENTS

This work was supported by the college studentsinnovation and entrepreneurship training project(201710622037); the Talent Project of Sichuan University ofScience & Engineering (2017RCL23); the Science Foundingof Artificial Intelligence Key Laboratory of Sichuan Province(2017RZJ03); the Opening Project of Sichuan ProvinceUniversity Key Laboratory of Bridge Non-destructionDetecting and Engineering Computing (2017QYJ03); the key laboratory of higher education of Sichuan Provincefor enterprise informationalization and Internet of things (No. 2017WYJ02).

REFERENCES

[1]. Lin, L. F., Lin, Y. J., Lin, Z. H., Chuang, L. Y., Hsu, W. C., & Lin, Y. H. (2018). Feasibility and efficacy of wearable devices for upper limb rehabilitation in patients with chronic stroke: a randomized controlled pilot study.European journal of physical and rehabilitation medicine,54(3), 388-396.

[2]. Adapa, A., Nah, F. F. H., Hall, R. H., Siau, K., & Smith, S. N. (2018). Factors influencing the adoption of smart wearable devices.International Journal of Human–Computer Interaction,34(5), 399-409.

[3]. Izmailova, E. S., Wagner, J. A., & Perakslis, E. D. (2018). Wearable devices in clinical trials: hype and hypothesis.Clinical Pharmacology & Therapeutics,104(1), 42-52.

[4]. Khalifa, S., Lan, G., Hassan, M., Seneviratne, A., & Das, S. K. (2018). Harke: Human activity recognition from kinetic energy harvesting data in wearable devices.IEEE Transactions on Mobile Computing,17(6), 1353-1368.

[5]. Kohani, M., Bhandare, A., Guan, L., Pommerenke, D., & Pecht, M. G. (2018). Evaluating Characteristics of Electrostatic Discharge (ESD) Events in Wearable Medical Devices: Comparison With the IEC 61000-4-2 Standard.IEEE Transactions on Electromagnetic Compatibility,60(5), 1304-1312.

[6]. Di Giminiani, R., Lancia, S., Ferrari, M., Quaresima, V., Vistisen, H. T., Kliltgaard, A., ... & Cardinale, M. (2018, June). A wearable integrated textile EMG and muscle oximetry system for monitoring exercise-induced effects: a feasibility study. In2018 IEEE International Symposium on Medical Measurements and Applications (MeMeA),pp. 1-5.

[7]. Kohzaki, H., Ishida, Y., & Fujita, Y. (2016). Use of wearable devices in medicine and in paramedical education and the need for training of medical data scientists.Information Engineering Express,2(2), 1-16.

[8]. Kim, Y., Lee, W., Raghunathan, A., Raghunathan, V., & Jha, N. K. (2015). Reliability and security of implantable and wearable medical devices. InImplantable Biomedical Microsystems,pp. 167-199.

[9]. He, D., & Zeadally, S. (2015). An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography.IEEE internet of things journal,2(1), 72-83.

[10]. Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2016). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography.Electronic Commerce Research,16(1), 113-139.

[11]. Liu, Z., Großschädl, J., Hu, Z., Järvinen, K., Wang, H., & Verbauwhede, I. (2017). Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things.IEEE Transactions on Computers,66(5), 773-785.

[12]. Reddy, A. G., Das, A. K., Yoon, E. J., & Yoo, K. Y. (2016). A secure anonymous authentication protocol for mobile services on elliptic curve cryptography.IEEE Access,4, 4394-4407.

[13]. Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication.Future Generation Computer Systems,81, 557-565.

Zouyu Xie" Wearable Medical Device Data Transmission System Based On Elliptic Curve Cryptography" American Journal of Engineering Research (AJER), vol.8, no.02, 2019, pp.90-94