# Secure Wearable Apps for Remote Healthcare Through Modern Cryptography

##### **Andric Li\*, Grace Luo\*\*, Christopher Tao\*\*\* ,Preston Lau \*\*\*\***

\* Department of Computer Science, UCSD

\*\* Department of Computer Science, U-Wisconsin-Madison

\*\*\* The Bishop’s School

\*\*\*\*Huawei

DOI: 10.29322/IJSRP.X.X.2018.pXXXX

<http://dx.doi.org/10.29322/IJSRP.X.X.2018.pXXXX>

***Abstract*-** Wearable devices like smartwatch, wrist band, fitnessins tracker, are designed to be light weight and comfortably worn close to human body. With the increased connectivity of wearable devices, they become part of solution for remote health care. For example, a smart watch measures and uploads patient’s vital signs to the cloud through network which is monitored by software backed with Artificial Intelligence. Any anomaly of a patient will be detected and alerted to healthcare professionals for proper disposal. Remote health benefits both patient and healthcare providers. Patient may avoid expensive in-patient care by choosing comfort of staying at home while being monitored after a surgery. Meantime, healthcare providers find remote healthcare effective to resolve challenges between limited resources and increasing population.

While remote health care through wearable devices are ubiquitous and affordable, patient privacy becomes a challenge. Patient should be concern about his or her privacy. Is my data stored in the cloud safe? Can an adversary accesses and manipulates my data for blackmailing? Hence, securing patient private information end-2-end becomes crucial. This paper explores solutions of applying modern cryptography to secure wearable apps and ensure patient private data is protected with confidentiality, integrity, and authenticity from wearable edge to cloud.

***Index Terms***- wearable apps, remote healthcare, cryptography, security

1. Introduction

While remote healthcare has become a compelling solution with the advent wearable devices, patient’s privacy must be properly addressed to ensure patient’s data are protected from any adversaries from the point when data are collected through a wearable or IOT device at the cloud edge to the point where data stored and retrieved by health care provider in a public cloud platform. Cloud service providers (CSPs) like Microsoft Azure or Google provide tools and capabilities to healthcare providers to secure user data after data have been uploaded. User privacy at the cloud Edge however, is out of protection scope of CSPs. The protection at the wearable devices where data are collected become the responsibility of the smart wearable apps. The good news is that modern cryptography adopted by cloud service providers can be leveraged to protect user data collection by smart wearable apps. The US National Institute of Standards and Technology (NIST) has published a set of cryptographic algorithms such as Advanced Encryption Algorithm (AES) for data encryption and Diffie-Hellman Key Exchange (DH) for pair-wise key establishment. These cryptographic algorithms facilitate smart wearable apps to establish a unique secure channel between the edge device and cloud healthcare database. Secure channel mutually authenticates a patient to the target healthcare database in the cloud and vice versa. In addition, secure channel derives a session key for subsequent data transfer, hence, patient data will be encrypted by a dedicated and unique key at the point data are collected and decrypted only at the target cloud database.

This research prototypes a secure smart watch app for health monitoring for remote patient care. This app illustrates how a secure channel is constructed using crypto APIs provided by Android Studio. This app demonstrates how patient data encrypted at the time data is collected from the sensor before sending the data to the remote server through an open network, and how the remote server decrypts the patent data with the assurance of data confidentiality, authenticity and integrity.

This paper consists of five sections as following:

1. Abstract
2. Introduction
3. Standards And Government Regulations
4. Cryptography for Remote Healthcare App
5. Demonstration of a Secure Smartwatch App
6. Conclusions and Future Research
7. Standards And Government Regulations

The US Health Insurance Portability and Accountability Act (HIPAA) is very strong about technical safeguards, as the standards developed for these represent healthy business practices for technology and related procedures and policies. As specified in the HIPAA § 164.312(e)(2)(ii):

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must: “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

This instruction from HIPAA seems vague and leaves quite some space for interpretation, because the RHIPAA rule allows companies to use any security measures that allow it to apply the standards reasonably and appropriately, to safeguard the electronic protected health information (EPHI). Meanwhile the European Union’s General Data Protection Regulation (GDPR) is more specific. In [article 32,](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3383-1-1) the GDPR specifies:

*“... the controller and the processor* ***shall implement appropriate technical and organisational measures*** *to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

a.) pseudonyms and encryption of personal data

b.) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

c.) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

d.) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. “

And in [recital 83](https://www.privacy-regulation.eu/en/recital-83-GDPR.htm) it further specified:  
*In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and* ***implement measures to mitigate those risks, such as encryption****. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. ...****”***

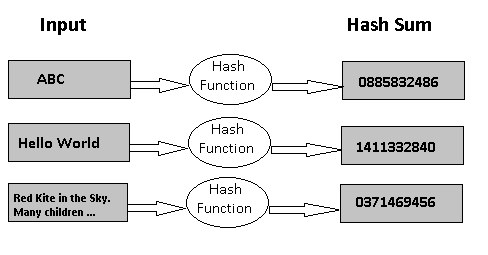
Although the GDPR aimed at protecting data privacy in the EU nations, the regulation applies to the entities wants to operates with EU, and hence has broader impact beyond EU.

1. Cryptography for Securing remote healthcare applications

It's the foremost preliminary step for proceeding with any research work writing. While doing this go through a complete thought process of your Journal subject and research for it's viability by following means:

1. Read already published work in the same field.
2. Goggling on the topic of your research work.
3. Attend conferences, workshops and symposiums on the same fields or on related counterparts.
4. Understand the scientific terms and jargon related to your research work.
5. Cryptography for securing remote healthcare applications

Modem cryptography can be leveraged to achieve the pseudonyms and encryption of personal data goal set forth by HIPPA and GDPR. Three classes of cryptographic algorithms and protocol are suitable for remote healthcare apps including Secure Hash Algorithm (SHA) for pseudonyms of personal data, Advance Encryption Standard in Galois/Counter Mode (AES-GCM) for data encryption, and Elliptic Curve Diffie-Hellman Key Exchange (ECDH) for establishing remote key pair.

SHA is a one-way compression function. SHA is known to be infeasible to modify a message without changing its digest. In addition, SHA is infeasible to generate another message matching a digest. Thirdly, SHA is infeasible to find two messages with an identical digest. These prominent features make SHA ideal to obfuscate patient IDs to form pseudonym which is unique to the patient and impossible to retrieve. The following example shows how a SHA produces pseudonyms.

AES-GCM is an authenticated encryption algorithm developed to protect data in transit. AES-GCM encryption produces cipher text through counter mode AES and a tag produced by a Galois field multiplier. Both the cipher text and the tag will be transmitted through open network. Upon arrival, the receiver decrypts the datagram cipher text, produces a fresh tag, and compares the local produced tag to the tag received. If there is any data tampering, a tag mismatch shall detect the anomaly. Subsequently, the driver erases the decrypted content and returns error status. Of course, in a normal case, tags match, hence, driver will render the plaintext. The following is an AES-GCM block diagram.

Input

Output

Key/IV

AES-CTR

GF Multiplier

Tag

AES-GCM requires a session key for data encryption. Session key can be established by ECDH protocol. ECDH is a key exchange protocol and developed to derive a common session key based on public/private key pair for two remote entities. Here is one example to illustrate how ECDH works. Assume Alice and Bob want to establish a session key, Alice and Bob agree on a set of predefined domain parameters including a generator called G.

Alice generates a private key dA through random number generator, and its corresponding QA

Bob generates a private key dB through its random number generator, and its corresponding QB

Alice and Bob exchange public key QA and QB through open network. Alice performs the following operation subsequently

Bob performs the following operation likewise

Note that CA and CB are identical, hence, CA and CB become the session key for Alice and Bob to encrypt and decrypt subsequent messages.

Now it is the time to articulate the research work with ideas gathered in above steps by adopting any of below suitable approaches:

## A. Bits and Pieces together ( Describe Android SDK and Crypto APIs)

In this approach combine all your researched information in form of a journal or research paper. In this researcher can take the reference of already accomplished work as a starting building block of its paper.

Jump Start

This approach works the best in guidance of fellow researchers. In this the authors continuously receives or asks inputs from their fellows. It enriches the information pool of your paper with expert comments or up gradations. And the researcher feels confident about their work and takes a jump to start the paper writing.

## B. Use of Simulation software

There are numbers of software available which can mimic the process involved in your research work and can produce the possible result. One of such type of software is Matlab. You can readily find Mfiles related to your research work on internet or in some cases these can require few modifications. Once these Mfiles are uploaded in software, you can get the simulated results of your paper and it easies the process of paper writing.

As by adopting the above practices all major constructs of a research paper can be written and together compiled to form a complete research ready for Peer review.

1. Simulation platform

The Android Studio is selected for the simulation because of its ease of development and rich platform ecosystem, it includes an Android Emulator that simulates Android devices on your computer so that you can test your application on a variety of devices and Android API levels without needing to have each physical device [quote].

The project simulation made use of the Android Emulation platform, created a Smart Watch Wear OS APP to run on the emulator, and a server function to run on the local computer. The smart watch implements a heartrate monitor function of the health service defined by the Wear OS, and makes use of the communication functions provided from the platform. Wear OS apps can make network requests. When a watch has a Bluetooth connection to a phone, the watch's network traffic generally is proxied through the phone.

When a phone is unavailable, Wi-Fi and cellular networks are used, depending on the watch hardware. The Wear OS platform handles transitions between networks. [quote] For design simplicity reason, the configuration in this project illustrates a system without a phone, the smartwatch communicates directly with the server, which is implemented using Python Script.

1. Healthcare Data encryption Simulation

The Android Studio already provided data protection at the transport functions, when the data is sent over the network. But this is not sufficient. This project illustrates the data encryption end-to-end from the application level. The intercepting points are carefully selected to introduce the secure channel establishment, and health data encryption-decryption.

….

1. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

The simulation demonstrated the data protection on the secure smart watch for health monitoring for remote patient care. This application illustrates how a secure channel is constructed using crypto APIs provided by Android Studio, how patient heart rate data is encrypted using the Wear OS API, before sending the data to the remote server through an open network, and how the remote server decrypts the patient's heart rate data with the assurance of data confidentiality, authenticity and integrity.

This simulation chose to establish the secure channel at the time of the smart watch – server connection establishment, and to perform the encryption and decryption upon every data transfer, which may add an insignificant power and latency to the communication.

As described in the HIPAA security standard § 164.312(e)(2)(ii):

“Adopting a single industry-wide encryption standard in the Security Rule would likely have placed too high a financial and technical burden on many covered entities. The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use.”

1. FUTURE STUDY

## Session management.

Since there is no private key shared in the process of setting up the secure channel or in the data exchange communication, there is no concern of secure key leaking in this case. However; it can be a subject for future study on the frequency to reestablish the secure channel between the wearable health device and the server or the cell phone. Since wearable devices are power and performance constrained, and the process of establishing secure channel, and encrypting measured data takes power and time, there should be consideration and trade-off analysis among power consumption, communication latency, and security.

Some examples could be, establishing the secure channel less frequent only once per wearable device or host cellphone reset; or establishing the secure channel very frequent at once per data communication; or something in between, periodically triggers the re-establishing of the secure channel based on events like timer.

Adding Mobile device in the system?

Regarding Integrity, the HIPAA specified:

“The Integrity standard requires a covered entity to:

“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.” ”

The covered entity must determine the security measures for to use in its organization. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Access controls should revolve around enabling the correct users to access only the necessary information needed to do their job: for example, a doctor reading patient wearable device data to monitor a sleep condition. It is essential that User identification is unique for tracking a user and their identity.

The data should be encrypted both in transit and at rest and has to be at least 128-bit. A unique encryption key should not be stored on the server.

To accomplish this, all data transmission points must be known and mechanisms must be used to provide encryption in transit and integrity verification. APPs are needed to support encryption and decryption using networking protocols. Services providing encryption include KMS, S3, RDS, EFS, EM, and IPsec. Keys must be rotated on a regular basis.

1. GET PEER REVIEWED

Here comes the most crucial step for your research publication. Ensure the drafted journal is critically reviewed by your peers or any subject matter experts. Always try to get maximum review comments even if you are well confident about your paper.

**For peer review send you research paper in IJSRP format to** [**editor@ijsrp.org**](mailto:editor@ijsrp.org)**.**

1. IMPROVEMENT AS PER REVIEWER COMMENTS

Analyze and understand all the provided review comments thoroughly. Now make the required amendments in your paper. If you are not confident about any review comment, then don't forget to get clarity about that comment. And in some cases there could be chances where your paper receives number of critical remarks. In that cases don't get disheartened and try to improvise the maximum.

**After submission IJSRP will send you reviewer comment within 10-15 days of submission and you can send us the updated paper within a week for publishing.**

This completes the entire process required for widespread of research work on open front. Generally all International Journals are governed by an Intellectual body and they select the most suitable paper for publishing after a thorough analysis of submitted paper. Selected paper get published (online and printed) in their periodicals and get indexed by number of sources.

**After the successful review and payment, IJSRP will publish your paper for the current edition. You can find the payment details at:** [**http://ijsrp.org/online-publication-charge.html**](http://ijsrp.org/online-publication-charge.html)**.**

Appendix

Appendixes, if needed, appear before the acknowledgment.

Acknowledgment

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments.

References

1. G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, *Linear Networks and Systems* (Book style)*.* Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.
5. E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” *IEEE Trans. Antennas Propagat.*, to be published.
6. J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” *IEEE J. Quantum Electron.*, submitted for publication.
7. Hipaa Security Series #4 - Technical Safeguards - Hhs.gov. [www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf](http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf).
8. “Art. 32 GDPR - Security of Processing.” GDPR.eu, 14 Nov. 2018, gdpr.eu/article-32-security-of-processing/.
9. “Art. 25 GDPR - Data Protection by Design and by Default.” GDPR.eu, 23 July 2020, gdpr.eu/article-25-data-protection-by-design/.
10. Reference section for simulation platform
11. Android Studio, from Android developer official website at <https://developer.android.com/studio>
12. Android Emulator, from Android developer official website at <https://developer.android.com/studio/run/emulator>
13. <https://developer.android.com/studio/run/emulator#wear-os-pairing>

Authors

**First Author** – Author name, qualifications, associated institute (if any) and email address.

**Second Author** – Author name, qualifications, associated institute (if any) and email address.

**Third Author** – Author name, qualifications, associated institute (if any) and email address.

**Correspondence Author** – Author name, email address, alternate email address (if any), contact number.