International Journal of Advanced Smart Convergence Vol.8 No.2 204-210 (2019)
http://dx.doi.org/10.7236/IJASC.2019.8.2.204

IJASC 19-2-25

An Efficient Multi-Layer Encryption Framework with Authentication for EHR in Mobile Crowd Computing

Rethina kumar[1], Gopinath Ganapathy[2], GeonUk Kang[3]

[1]*Assistant Professor, Dept of Information and Communication, Dong Seoul University, Korea*
Research Scholar, Bharathidasan University, India
[2]*Registrar, Bharathidasan University, India*
[3]*Graduate Student, Data Science Convergence, Sung Kyun Kwan University, Korea*
kumarrethina@yahoo.com, brkumar76@yahoo.com

Abstract

Mobile Crowd Computing is one of the most efficient and effective way to collect the Electronic health records and they are very intelligent in processing them. Mobile Crowd Computing can handle, analyze and process the huge volumes of Electronic Health Records (EHR) from the high-performance Cloud Environment. Electronic Health Records are very sensitive, so they need to be secured, authenticated and processed efficiently. However, security ,privacy and authentication of Electronic health records(EHR) and Patient health records(PHR) in the Mobile Crowd Computing Environment have become a critical issue that restricts many healthcare services from using Crowd Computing services .Our proposed Efficient Multi-layer Encryption Framework(MLEF) applies a set of multiple security Algorithms to provide access control over integrity, confidentiality ,privacy and authentication with cost efficient to the Electronic health records(HER)and Patient health records(PHR). Our system provides the efficient way to create an environment that is capable of capturing, storing, searching, sharing, analyzing and authenticating electronic healthcare records efficiently to provide right intervention to the right patient at the right time in the Mobile Crowd Computing Environment.

Keywords*: Mobile crowd computing, Healthcare Security, Medical Image Encryption, encryption algorithm, Digital Signature, hashing algorithm*

1. Introduction

Mobile Crowd Computing needs high computing power for the huge volume of sensitive medical data and they need large storage for storing both electronic medical data and their outcomes. Our research system provides a multi-layer encryption framework (MLEF) that involves multiple cloud environment. They are Data Storage Cloud, Security Cloud, Application Cloud with different algorithms which performs different applications and it also involves members such as mobile users, crowd sourcing, data owners, data users, cloud servers, experts, Doctors and authority globally. We try to provide an efficient solution

Manuscript Received: June. 2, 2019 / Revised: June. 8, 2019 / Accepted: June. 13, 2019
Corresponding Author: kumarrethina@yahoo.com
Tel: +82-31-720-2242
Dept of Information and Communication, Dong Seoul University, Korea & Research Scholar, Bharathidasan University, India

to the problem of sharing important EHR/ PHR information and propose a secure system with integrated mechanism by ensuring data privacy with authentication.

1.1 Cryptography

In cryptography, encryption is the process of encoding a message or information in a way that only authorized person can access it using a set of keys. The private key is a random hexadecimal number that must be kept private by the account holder. A public key is another hexadecimal number which can be shared publicly.

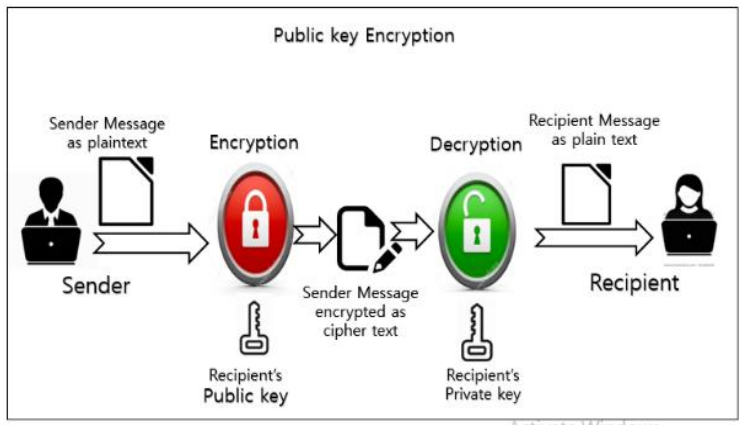

Figure 1. Public-key cryptography or asymmetric cryptography

1.2 Digital Signature and Hash Function

The digital signature is a process to validate the authenticity of any electronic information. To create a digital signature, the signing software creates a one-way hash of the data to be signed. The private key is then used to encrypt the hash. This encrypted hash plus other information like the hashing algorithm used is the digital signature. A digital signature with public key cryptography securing a message is created in the following way. First, the message is digitally signed Then, this bundle is encrypted with the sender's private key and again with the receiver's public key. The formation of public key with digital signature look like public_key_of_recipient(private_key(message_hashing(message) + message + type of hashing algorithm)).

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. The hash function is used to index the original value or key and then used later each time the data associated with the value or key is to be retrieved. Thus, hashing is always a one-way operation. Hashing is used to retrieve data faster and hashing is also used to encrypt and decrypt digital signatures. The digital signature is transformed with the hash function and then both the hashed value (known as a message-digest) and the signature are sent in separate transmissions to the receiver. Using the same hash function as the sender, the receiver derives a message-digest from the signature and compares it with the message-digest it also received. (They should be the same.)

Table 1. Hash Function Property used in cryptography.

Hash function	Hash length	Secure
md5	128 bits (32 symbols)	No *
ripemd160	160 bits (40 symbols)	Yes
sha1	160 bits (40 symbols)	No *
sha256	256 bits (64 symbols)	Yes
keccak-256	256 bits (64 symbols)	Yes

Table 2. Hash / MAC / Digital Signature - Security Goals.

Cryptographic primitive Security Goal	Hash	MAC	Digital signature
Integrity Authentication Non-repudiation	Yes No No	Yes Yes No	Yes Yes Yes
Kind of keys	none	symmetric keys	asymmetric keys

A hash chain is the successive application of a cryptographic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence.

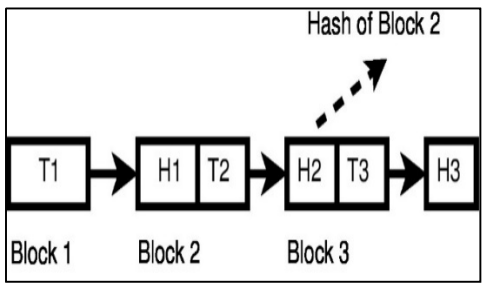

Figure 2. Hash chain Block Diagram

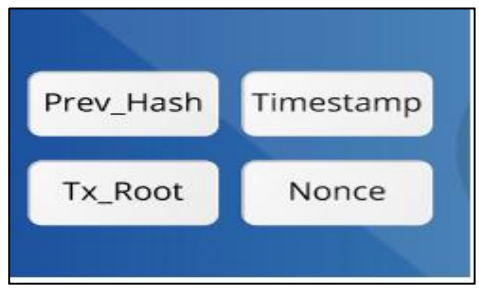

Figure 3. Block Elements

1.3 One-Time Pad

The theory behind the OTP is that the encryption key has at least the same length as the actual message (i.e. the plaintext) and consists of truly random numbers. Each letter of the plaintext is 'added' to one element from the OTP using modulo-addition. This results in a cipher text that has no relation with the plaintext when the key is unknown. At the receiving end, the same OTP is used to retrieve the original plaintext.

1.4 DICOM

Digital Imaging and Communications in Medicine(DICOM) is the most commonly adopted system to access and share the medical images in cloud environment which is capable of providing fully digital images with high resolution. Using DICOM, the images produced by medical imaging devices like CT Scan, MRI Scan, X-Ray Machine, Ultrasound can be integrated into picture archiving and

communication systems (PACS) and can be exchanged in the cloud environment. The DICOM standard not only encodes the image but also a set of metadata and attributes, that describe the images.

In our research, we try to provide an effective solution to the problem of sharing the electronic medical information such as EHR/PHR to gain knowledge in medical information, clinical trials, research, medical images and propose a secured, integrated and authenticated mechanism while ensuring Integrity, Authentication, Non-repudiation with efficient medical related information with timely and efficient access to EHR/PHR and medical related information.

2. Related Research

K. Zheng et, al [2013] introduce Honeybee; a crowd computing framework for mobile devices. Honeybee enables mobile devices to share work, utilize local resources and human collaboration in the mobile context. It employs 'work stealing' to effectively load balance tasks across nodes that are a priori unknown and describe the design of Honey bee, and report initial experimental data from applications implemented using Honeybee [1]

Rathod et, al [2016] review a crowd computing for mobile devices. Here they explore this concept of 'work stealing' for crowd computing on an opportunistic network of mobile devices, for both machine and human computation and also present experimental data and discuss the findings. [2]

M. Somasundaram et, al [2011] describes about the management of medical image data in a cloud computing environment with access to mobile users through a mobile application to help the patients and doctors to view patient health records and prescriptions on their handheld devices that supports Android OS. The application that has been effectively implemented allows a flexible medium for patients to access vital health records at their convenience, without a need to visit the hospital to view the same. The application is an advantage to people residing in remote areas and who cannot access hospitals in cities at tease. [3]

Derek et al [2010], introduce and motivate crowd computing, which combines mobile devices and social interactions to achieve large-scale distributed computation. An opportunistic network of mobile devices offers substantial aggregate bandwidth and processing power. Here analyze encounter traces to place an upper bound on the amount of computation that is possible in such networks and also investigate a practical task-farming algorithm that approaches this upper bound, and show that exploiting social structure can dramatically increase its performance. [4]

ChengYe et al [], we introduce a crowdsourcing framework to support the annotation of medical datasets, and they further demonstrate a workflow for crowdsourcing clinical chart reviews including (1) the design and decomposition of research questions; (2) the architecture for storing and displaying sensitive data; and (3) the development of tools to support crowd workers in quickly analyzing information from complex datasets. [5]

Imdat As et al [], discuss the methods and techniques of architectural crowdsourcing and illustrate the processes and outcomes through a series of projects: a remodelling project for a closet; an interior design challenge for a dining space; and a layout problem for an apartment complex. We will then evaluate the protocol and outcome of architectural crowdsourcing, and convey the professional and popular media response to this new method of architectural design acquisition. [6]

Kerri Wazny, discuss the Eight areas where crowdsourcing has been used in health were identified: diagnosis; surveillance; nutrition; public health and environment; education; genetics; psychology; and,

general medicine/other. Many studies reported crowdsourcing being used in a diagnostic or surveillance capacity. Crowdsourcing has been widely used across medical disciplines; however, it is important for future work using crowdsourcing to consider the appropriateness of the crowd being used to ensure the crowd is capable and has the adequate knowledge for the task at hand. Gamification of tasks seems to improve accuracy; other innovative methods of analysis including introducing thresholds and measures of trustworthiness should be considered. [7]

3. Proposed System Frame Work

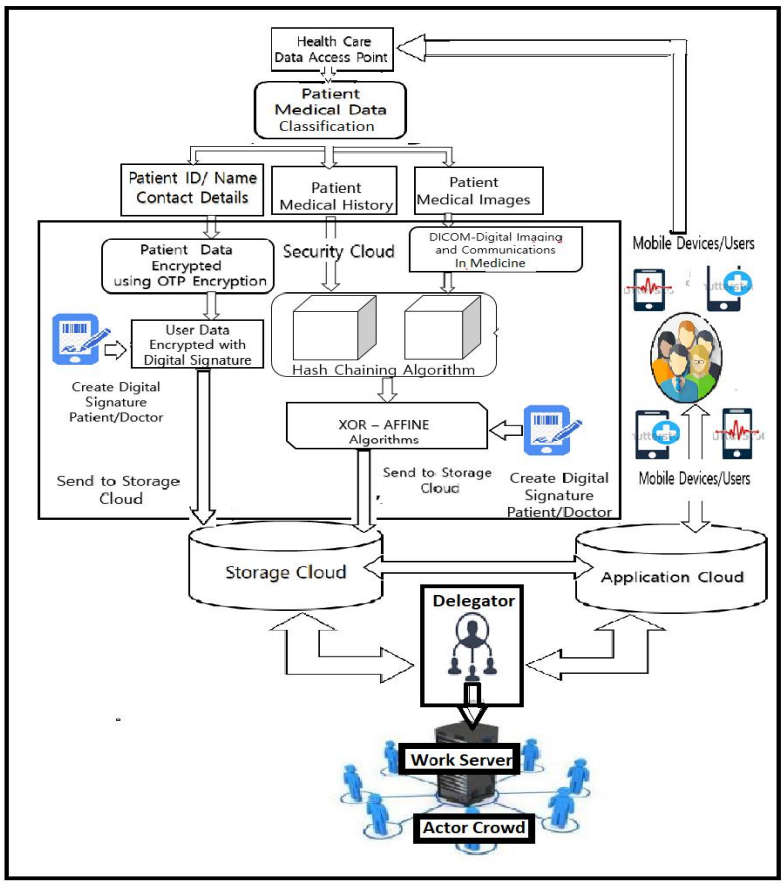

Figure 4. An Efficient Multi-Layer Encryption Framework with Authentication

The proposed framework involves different functional Clouds that performs different applications. The Security cloud consists of different types of security algorithm that encrypts the Electronic Health Records / Personal Health Records and then this medical data set is sent to Storage cloud which stores this encrypted medical information. Application cloud contains the main algorithm to run the calculation and services provided by the applications and then form the integrated systems from the authorized parties. In our proposed frame work the patient medical data is classified into multiple blocks (Block 1, Block 2, Block 3). Each block is encrypted and decrypted with multi-layer algorithms. Block 1 is encrypted with One Time Pad(OTP) embedded with digital signature. Block 2 and Block 3 uses multi-layer encryption (hash chain, XOR-AFFINE) with digital signature. Digital signature plays a major role in validating EHR/PHR. Our proposed frame work is explained in the algorithm (3.1).

3.1 Algorithm for the Proposed Frame Work. (Fig. 4)

Step 1: Initialize the system process through health care data access point.
Step 2: Patient medical data is classified into 3 different blocks.
Step 3: Block 1 contains patient id/name/contact information and these data's are very sensitive.
Step 4: Block 2 contains patient medical history.
Step 5: Block 3 contains patient medical images with its metadata.
Step 4: Block 1 contains very sensitive patient information so they are encrypted separately with one-time pad (OTP) encryption algorithm.
Step 4.1: Then the Patient/Doctor creates a digital signature by authorized process to authenticate the patient information.
Step 4.2: Then the Digital signature is embedded with the encrypted patient digital data.
Step 4.3: Send this Block 1 Patient data (digital signature + encrypted) to the storage cloud separately to ensure the sensitivity.
Step 5: Block 2 Contains patient medical history and this data is sent to hash chaining block.
Step 6: Block 3 contains the patient medical images and its meta data is embedded with DICOM.
And then sent to hash chaining.
Step 6.1: The hash chaining algorithm is performed in Block 2 and Block 3.
Step 6.2: Then this set of data is encrypted with multi-layer XOR-AFFINE encryption.
Step 6.3: With (step 6.2) encrypted electronic medical data the corresponding authorized digital signature is embedded and then sent to the storage cloud.
Step 7: The storage cloud contains the corresponding decryption process for the above encrypted electronic health records and performs the decryption with authorized digital signature once they are valid.
Step 8: Application cloud that contains the main algorithm will initiate and then form the integrated systems from the authorized parties.
Step 9: Electronic health records from the storage cloud given to Delegator and queues the work and send it to Work server.
Step 10: Work Server get the work from Delegator and given to Mobile Crowd.
Step 11: Crowd member analyze the existing data and knowledge present and sent back to work server.
Step 12: Work server Collaborate the knowledge and given to Delegator.
Step 13: Delegator gives back the electronic health records with Crowd Knowledge.
Step 14: Application cloud does the calculation with algorithm to find the relation with crowd knowledge and electronic health records and find the optimal solution in the form ofrecommendation.
(Cost efficient, Best hospital, Medicine, Treatment awareness, suitable best doctors, alternative like wise.)

4. Conclusions and Future Enhancement

Our proposed framework provides authentication of Electronic Health Record / Personal Health Record with optimal solution in the form of recommendation. (Cost efficient, Best hospital, Medicine, Treatment awareness, suitable best doctors, alternative like wise.) in mobile crowd computing environment. The framework provides a high level of Integrity, Authentication, Non-repudiation, Interoperability, and sharing of EHR / PHR among healthcare Organization, Patients and Practitioners, Researchers globally. The mobile crowd computing allows fast Internet access and mobile internet(4G/5G) for sharing EHR / PHR by the authenticated users. The proposed

frame work analyzes patient data to provide right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of the EHR / PHR. and helps the healthcare organization to provide high quality and cost-effective treatment using this combination of crowd computing and mobile computing technologies. In the future we plan to design and implement Mobile Crowd Computing for Medical Health Information Technologies based on our proposed framework.

References

[1] K. Zheng, M. Li, and H. Jiang (Eds.), Honeybee: A Programming Framework for Mobile Crowd Computing MOBIQUITOUS", 2013, LNICST 120, pp. 224–236, 2013.
[2] Ivan Stojmenovic, ": Mobile Cloud and Green Computing", Procedia Computer Science,2012.
[3] M. Somasundaram, S.Gitanjali, T.C.Govardhani, G. Lakshmi Priya and R. Sivakumar, "Medical Image Data Management System in Mobile Cloud Computing Environment", IPCSIT, 2011.
[4] Derek G. Murray, Eiko Yoneki Jon, Crowcroft Steven Hand, "The Case for Crowd Computing", MobiHeld 2010.
[5] Cheng Ye, Joseph Coco, Anna Epishova, Chen Hajaj, Henry Bogardus, Laurie Novak, Joshua Denny, Yevgeniy Vorobeychik, Thomas Lasko, Bradley Malin, Daniel Fabbri, "A Crowdsourcing Framework for Medical Data Sets", Vanderbilt University, Nashville, TN, US
[6] Imdat As, Maria Angelico, "CROWDSOURCING ARCHITECTURE: A DISRUPTIVE MODEL IN ARCHITECTURAL PRACTICE", University of Hartfor
[7] Kerri Wazny, "Applications of crowdsourcing in health: an overview", global journal of health.
[8] Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure Isma Masood ,1 YongliWang,1 AliDaud,2 NaifRadiAljohani,3 andHassanDawood4 Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 2143897, 23 pages
[9] Ahmad Habboush, Multi-Level Encryption Framework (IJACSA) International Journal of Advanced Computer Science and Applications, | P a g e -130, Vol. 9, No. 4, 2018.
[10] Medical Image Encryption: An Application for Improved Padding Based GGH Encryption Algorithm Massoud Sokouti1, Ali Zakerolhosseini2 and Babak Sokouti3, * -- Article in The Open Medical Informatics Journal · 2016
[11] Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing Aymen Mudheher Badr 1, Yi Zhang 1 and Hafiz Gulfam Ahmad Umar 2, -- MDPI 2019.
[12] International Conference on Medical Imaging Understanding and Analysis 2016, Loughborough, UK-- Security of multi-frame DICOM images using XOR encryption approach Q. N. Natsheh*, B. Li, A. G. Gale.
[13] A Survey about Consensus Algorithms Used in Blockchain- Giang-Truong Nguyen* and Kyungbaek Kim Inf Process Syst, Vol.14, No.1, pp.101~128, February 2018 ISSN 1976-913X (Print).
[14] DIP Using Image Encryption and XOR Operation Affine Transform Anurag Singh1, Dr. Namrata Dhanda2 - (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar –Apr. 2015), PP 07-15
[15] Dirk Rijmenants, Secure Communications with the One Time Pad Cipher Version 6.2, 18 December 2014.
[16] One-time password based on hash chain without shared secret and re-registration- Chang-Seop Park Elsevier - 19 February 2018 Available online 28 February 2018.